NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

UNMANNED TACTICAL AUTONOMOUS CONTROL AND COLLABORATION THREAT AND VULNERABILITY ASSESSMENT

by

Louis T. Batson V
Donald R. Wimmer Jr.

June 2015

Thesis Advisor: Dan Boger
Second Reader: Scot Miller

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
UNMANNED TACTICAL AUTONOMOUS CONTROL AND COLLABORATION THREAT AND VULNERABILITY ASSESSMENT

5. FUNDING NUMBERS

6. AUTHOR(S) Louis T. Batson V and Donald R. Wimmer Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Information systems designed and developed without considering security and potential threats create avoidable risks to the United States and the Department of Defense (DOD). Unmanned Tactical Autonomous Control and Collaboration (UTACC) is a ground-breaking and original approach to using systems autonomy to augment and improve the intelligence, surveillance, and reconnaissance process. However, UTACC will fail to accomplish that task if the system is not built with security in mind from the outset. To improve the security of UTACC, this thesis conducts an analysis to identify threats and vulnerabilities in the system's concept. The goal of this analysis was to mitigate threats and enable mission success to UTACC-supported missions. During the initial research, a framework for threat and vulnerability analysis was developed based on The National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) and DOD's Information Assurance Certification and Accreditation Process (DIACAP). This framework was used to create a threat template to analyze each threat facing UTACC and UTACC's inherent vulnerabilities. The templates also include technical and non-technical security control strategies to mitigate each of the vulnerabilities within UTACC.

14. SUBJECT TERMS UTACC, autonomy, information assurance, mission assurance, network security	**15. NUMBER OF PAGES** 175
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

UNMANNED TACTICAL AUTONOMOUS CONTROL AND COLLABORATION THREAT AND VULNERABILITY ASSESSMENT

Louis T. Batson V
Captain, United States Marine Corps
B.A., The Citadel, 2008

Donald R. Wimmer Jr.
Captain, United States Marine Corps
B.S., Park University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2015

Author: Louis T. Batson V.
Donald R. Wimmer Jr.

Approved by: Dr. Dan Boger
Thesis Advisor

Scot Miller
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information systems designed and developed without considering security and potential threats create avoidable risks to the United States and the Department of Defense (DOD). Unmanned Tactical Autonomous Control and Collaboration (UTACC) is a ground-breaking and original approach to using systems autonomy to augment and improve the intelligence, surveillance, and reconnaissance process. However, UTACC will fail to accomplish that task if the system is not built with security in mind from the outset. To improve the security of UTACC, this thesis conducts an analysis to identify threats and vulnerabilities in the system's concept. The goal of this analysis was to mitigate threats and enable mission success to UTACC-supported missions. During the initial research, a framework for threat and vulnerability analysis was developed based on The National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) and DOD's Information Assurance Certification and Accreditation Process (DIACAP). This framework was used to create a threat template to analyze each threat facing UTACC and UTACC's inherent vulnerabilities. The templates also include technical and non-technical security control strategies to mitigate each of the vulnerabilities within UTACC.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACE	aviation combat element
AGL	above ground level
ARP	address resolution protocol
ARPANET	Advanced Research Project Agency Network
ATO	Air Tasking Order
AVO	aerial vehicle operator
C2	command and control
CCI	Controlled Cryptographic Items
CNSSI	Committee on National Security Systems Instruction
COMSEC	communications security
COMPUSEC	computer security
COTS	commercial off the shelf
DIACAP	DOD Information Assurance Certification Accreditation Process
DOD	Department of Defense
DoN	Department of the Navy
DASC	Direct Air Support Center
EHF	extremely high frequency
EKMS	Electronic Key Management System
EM	electromagnetic
EO	electro-optical
EOD	explosive ordinance disposal
ES	enterprise system
EW	electronic warfare
FAC	forward air controller
FFRDC	Federally Funded Research Development Center
FIPS	Federal Information Processing Standards
FMF	Fleet Marine Force
FMO	future maritime operations
GCS	ground control station
HMI	human machine interaction

HVT	high value target
IA	information assurance
IAC	information assurance controls
IED	improvised explosive device
IFF	identify friend or foe
INFOSEC	information security
IP	Internet protocol
IR	infrared
IS	information system
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
LCAC	landing craft air cushion
LFOC	Landing Forces Operations Center
LZ	landing zone
MAC	media access control
MAGTF	Marine Air Ground Task Force
MC	mission commander
MCWL	Marine Corps Warfighting Laboratory
MIL-STD	military standard
NAI	named area of interest
NATOPS	Naval Aviation Training and Operating Procedure Standardization
NDP	Naval Doctrinal Publication
NIST	National Institute of Standards and Technology
NPS	Naval Postgraduate School
NSA	National Security Agency
PIN	personal identification number
RF	radio frequency
RFC	request for comment
RMF	risk management framework
SATCOM	satellite communication
SIPRNET	Secret Internet Protocol Router Network
SOP	standard operating procedure

SSN	Social Security number
STUAS	Small Tactical Unmanned Aerial System
TALS	tactical automated landing system
TTP	tactics, techniques, and procedures
UAS	unmanned aerial system
UAV	unmanned aerial vehicle
UGV	unmanned ground vehicle
UHF	ultra high frequency
US	United States
USMC	United States Marine Corps
UTACC	Unmanned Tactical Autonomous Control and Collaboration
VANET	vehicle area network
VLAN	virtual local area network
VMU	Marine Unmanned Aerial Vehicle Squadron

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Unmanned Tactical Autonomous Control and Collaboration (UTACC) system faces many diverse threats and is vulnerable on various fronts, but by applying security mitigation strategies this autonomous technology may be useful for the Marine Corps Warfighting Lab (MCWL). MCWL's mission is to "rigorously explore and assesses Marine Corps service concepts using an integral combination of wargaming, concept-based experimentation, technology assessments, and analysis to validate, modify, or reject the concept's viability, and identify capability gaps and opportunities, in order to inform future force development" [1]. The current squad level conceptual framework for the UTACC system neglects to address the inherent Information Assurance (IA) and Electronic Warfare (EW) concerns raised in modern warfare. Whitsett states that the initial survivability and IA of information systems must be identified, and a mitigating strategy must be validated before the development process begins [2]. The underlying question for this research is assessing the threats and vulnerabilities of the current UTACC concept of operations.

Identifying the internal and external threats that could affect the survivability and information assurance of the UTACC system will serve as a precursor to identify vulnerabilities and nullify them. This project can contribute to validate, modify, or reject the viability of a team level model of the UTACC system.

By utilizing key concepts from Information Technology (IT) literature, the authors analyze threats and vulnerabilities inherent within the UTACC system. This analysis is conducted by creating a threat template to evaluate the UTACC system. The template categorizes each threat, outlines related history, defines each threat, explains the potential impact to information held by UTACC, and provides the authors' relevant assumptions. Once identified, threats and vulnerabilities are assigned recommended security control strategies to mitigate the risks associated with each. As the UTACC system is not a tangible asset yet, the analysis is not conducted on the actual system.

The authors assessed 29 threats related to UTACC. The 29 threat templates are included in appendices A-CC. These threats were identified from the people, technology, and operations threat areas found in the Cyber Matrix [3]. In-depth analysis of the results revealed additional patterns. These patterns show some threats involving a malicious actor and others do not, some exist within the UTACC's operational organizations, some include the technology of UTACC itself, some exist against the design and integration of the UTACC system, and some arise against the employment of UTACC.

At the outset of research the anticipated areas of UTACC system vulnerability were within the system itself, the environment in which the system will be employed, and within the employing agency. After conducting our analysis two distinct patterns emerged. The first pattern categorizes vulnerabilities by the presence or absence of a kinetic or cyber malicious actor. Half of the analyzed threats contain a malicious actor; the rest exist within the employing organization, in the operating environment, or solely in the technology of UTACC. The second pattern relates to when in the life cycle threats emerge. The UTACC system is most vulnerable to threats during system employment and during design or development, and less vulnerable to threats during fielding, demonstration, and training. These patterns are key to understanding when the UTACC system is vulnerable and when security controls need to be added to the system.

Security controls are recommended as a starting point for the mitigation of each threat. These are essential to the success of the UTACC system project. Security Controls are sorted into non-technical and technical controls; they are not exhaustive, and do not include mitigation strategies at the component level specific to UTACC. A subset of security controls repeated through a majority of threats and therefore were identified as important to the success of the system.

The following security controls are recommended in the non-technical category:

- Policies, procedures and publications must be analyzed to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
- The UTACC system security policies and procedures must be developed to meet the requirements of the DOD and USMC. Ensure the UTACC system

completes the DIACAP process, which ensures the system meets DOD requirements for IA.

- Adherence to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
- Training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
- Extensive testing with operational units.

The following technical security controls are recommended:

- Remote zeroing of software, data, and cryptographic material.
- Employ tamper resistant technology.
- Independent UGV and UAV operations.
- Redundant and encrypted C2 and data links spread across the EM spectrum.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

The UTACC system, regardless of component configuration, will provide information to decision makers and the assurance of the information should be a responsibility of all parties involved with the UTACC system. In the design phase, engineers and program managers need to understand and plan for information assurance within the UTACC system. UTACC is on the cutting edge of technology in regards to information systems, but requires the same levels of protection and inherent responsibility to be effectively developed.

List of References

[1] Marine Corps Warfighting Lab Mission Statement. (n.d.). Marine Corps Warfighting Laboratory. [Online]. Available: http://www.mcwl.marines.mil. Accessed Apr. 1, 2015.

[2] Whitsett, J. W. Security of the User Centric Cloud. M.S. Thesis, Dept. Cyber Academic Group, Naval Postgraduate School, Monterey, Ca, March 2014.

[3] “Network Security Core Principles,” class notes for Network Security, Dept. of Computer Science, Naval Postgraduate School, Monterey, Ca, summer 2014.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Without ideas, effort, and assistance provided by our thesis advisor and second reader, Dr. Dan Boger and Scot Miller, this thesis would not have been possible. The authors would like to thank our families for continued support and sacrifice throughout the process. The authors would also like to thank the professors at the Naval Postgraduate School who provided endless amounts of support, ideas, and guidance that enabled the completion of this project. Finally, we would like to thank Chloe Woida at the Graduate Writing Center for her patience, guidance, and humor while editing our thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This thesis expands upon work already initiated on the Unmanned Tactical Autonomous Control and Collaboration (UTACC) system concepts and proposes how to incorporate a threat and vulnerability assessment to the system in the early developmental stages.

A. RESEARCH SPONSOR, OBJECTIVE AND RESULTS

The Marine Corps Warfighting Lab (MCWL) is the sponsoring command for the Unmanned Tactical Autonomous Control and Collaboration (UTACC) system. This initiative is a System of Systems that includes both air and ground components that aim to provide intelligence, surveillance, and reconnaissance (ISR) in support of a Marine Corps unit. The intention of this thesis is to perform a threat and vulnerability assessment of the UTACC system during the design, development, procurement and operational employment phases. Our team will offer mitigating strategies and concepts to each individual threat and vulnerability. The authors have operational experience with current unmanned aerial systems and cyber-security threats, but have no experience with a system this technologically advanced. This research is a broad look into many plausible threats and the UTACC system's vulnerability to each threat. Mitigating techniques will be comprised of best practices, policy, doctrine and procedures set forth by the Department of Defense (DOD), United States Marine Corps (USMC), and other government agencies.

Our thesis will aim to identify ways that system design, operational employment, and the enemy pose a threat to the UTACC system. The following research questions will be addressed in our thesis:

- What threats exist that have the potential to affect the UTACC?
- What vulnerabilities are inherent in the UTACC concept?
- What can be done to mitigate those threats and vulnerabilities within UTACC?

B. BENEFITS TO THE MARINE CORPS WARFIGHTING LAB

As technology continues to advance, systems like UTACC present an opportunity for the Marine Corps to expand their capabilities with autonomous systems. Threat and vulnerability assessments along with the related mitigating techniques, like those found in this thesis, will give a foundation for the MCWL to measure any autonomous system. A threat and vulnerability assessment of the UTACC system will identify potential friction points for developers and decision makers. This assessment will aid the MCWL in developing policies, procedures, and standards to develop an operationally capable, safe and secure system for Marines to employ in combat. Autonomous systems, like the UTACC, increase threat avenues for our enemies to exploit vulnerabilities. Identifying these threats and vulnerabilities before system development will aid in developing requirements for both the UTACC system and other autonomous systems.

C. RESEARCH METHODOLOGY OVERVIEW

As a small part of the UTACC project, this thesis will utilize key concepts from Information Technology (IT) literature for analyzing vulnerabilities inherent within the UTACC system. The analysis will be conducted by creating a threat template to evaluate the UTACC system and reveal vulnerabilities. As the UTACC system is not a tangible asset yet, the analysis will not be conducted on the actual system. After the analysis, this thesis will present security guidelines to mitigate the risks associate with each of the threats. Further research opportunities will be provided with different threat mitigation plans.

D. RELATED WORK

This thesis complements one other thesis in the UTACC program. That thesis, authored by Chhabra, Keim, and Rice, and in progress at the time of this writing, focuses on the UTACC system concept of operations and employment within the USMC. As the UTACC system has not been created yet, very little overlap occurs between the theoretical design and autonomous mapping that their thesis includes and the threat and vulnerability assessment in this thesis.

E. THE NEED FOR A THREAT AND VULNERABILITY ASSESSMENT

The unique and technical nature of the UTACC system opens the door for new threats and vulnerabilities. A wide range of threats are capable of impacting the UTACC system. These threats may arise due to the technology utilized by the system; the people designing, procuring, employing, and maintaining the system; and the system's operational environment. Threats that will target the UTACC system may require a wide range of security policies and procedures that must be addressed prior to employment.

F. ROAD MAP

This thesis presents a broad spectrum of threats and vulnerabilities with various effects on the UTACC system. The focus is on threats to the structure and implementation. This thesis is written so that the vulnerabilities and their recommended security control strategies can be applied to other autonomous systems with a similar purpose to UTACC. However, the intended audience is those designing UTACC.

There is a five-chapter structure for this thesis. Chapter I presents an overview of the thesis sponsor, concepts, research methodology, problem, and related work. The Literature Review in Chapter II defines the concepts necessary to conduct the threat and vulnerability analysis. Chapter III discusses the creation of a threat template for use in the analysis of each threat, and the threat selection process. Each section of the threat template is defined and discussed in this chapter as well. The analysis of one threat and vulnerability assessment is covered in Chapter IV with the remainder of the threats included as appendices. Chapter V will present conclusions and recommendations for further research.

The following is a summary of the chapter descriptions:

- Chapter I introduces the UTACC sponsor, concepts, research methodology, problem, and previous work.
- Chapter II provides the literature review of concepts, terms and academic work utilized to conduct this assessment.
- Chapter III covers the creation and areas of the threat template.

- Chapter IV analyzes one threat template in detail with discussion on each section of the template.
- Chapter V will provide our conclusions, answer our research questions, and provide any unexpected observations and recommendations for future UTACC work

II. LITERATURE REVIEW

This chapter reviews the concepts and terms required to understand information systems and network security principles. These concepts and terms are gathered from various publications and policies published by the U.S. government and academia. Although the Unmanned Tactical Autonomous Control and Collaboration (UTACC) system utilizes emerging technology and operational concepts, the UTACC system is an information system because it aids in the decision making process. An integration of people, doctrine, technology, and information allows a commander to gain situational awareness, make decisions, and implement those decisions [1]. First, this chapter introduces the basic concepts and terms related to Information Assurance (IA), which is the fundamental aspect of network security [2]. Once the concepts of IA are covered in detail, the threats to IA are discussed by analyzing all the elements of the cyber security matrix.

IA is an essential facet of network security and by extension is vital to the UTACC system [2]. The concepts of confidentiality, integrity, availability, authentication, and non-repudiation will be the guiding principles of the UTACC achieving IA. Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) requirements will guide the UTACC system assessment. The Department of Defense Instruction (DoDI) 8510.01 lays out the framework for Information Technology (IT) System risk management, DIACAP instructions and Department of Defense (DOD) policies for Information Technology (IT) [3]. An additional layer of analysis exists for UTACC due to its classification as a national security system. Understanding these concepts, processes, and procedures is critical in the evolution of the UTACC system to be employed by Marines on a future battlefield.

The mission of the UTACC system is to increase situational awareness through the sharing of relevant information, which is translated into knowledge by Marines. Knowledge Management is the integration of *people* through *technology* to enable the exchange of *operationally* relevant information to increase performance [4]. People,

technology, and operations are nested in the cyber security matrix as surface areas for threats and must be completely understood and will be defined in relation to information and information systems. The overarching concept of threats and their relation to information and information systems must be completely understood to attain IA. Vulnerabilities enable a vector for a threat to exploit information systems and must be elucidated. A security control enables the mitigation of a vulnerability to achieve IA. Systems security via computer security (COMPUSEC), Communications Security (COMSEC), and Information Security (INFOSEC) will guide us in the development of mitigation strategies for the UTACC system [5].

A. INFORMATION ASSURANCE

IA is a vital aspect of computer security, network security, communication security (COMSEC), and cryptographic systems [6]. IA is critical in enabling systems, such as the UTACC, to operate independently or in a networked environment. IA produces and defines procedures to protect signals, bits, and data as they traverse between systems or networks, enabling a decision maker to view information. The UTACC system, regardless of component configuration, will provide information to decision makers and the assurance of the information should be a responsibility of all parties involved with the design and development. DOD information systems require the same levels of protection and inherent responsibility to be effectively developed [7]. The National Security Agency (NSA) states that "information assurance is achieved when information and information systems are protected against such attacks through the application of security services such as availability, integrity, authentication, confidentiality, and non-repudiation" [8].

The definition of Information Assurance (IA) is the means by which UTACC will be evaluated for utility and risk management techniques. A review of the Committee on National Security Systems Instruction (CNSSI) 4009 provides a full definition of information assurance:

> Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of

> information systems by incorporating protection, detection, and reaction capabilities. [6]

The importance of IA has led to the establishment of the DIACAP that will maintain the information assurance posture of the system throughout the entire life cycle of said system. The purpose of IA is not perfect security, which cannot be attained, but a risk management strategy for each information system. Through this process of certification and accreditation assurance is attained. An individual will accept responsibility for the system and maximize security controls to reduce vulnerabilities.

The UTACC system should provide accurate information. The product of accurate information is a decision, thus the need to protect, assure, and reduce vulnerabilities of the information and information system, which is the end state of information assurance. “Information” has many definitions within military and civilian sectors and a comprehensive look at this term will allow an examination into the importance of the term. This will enable us to develop the concept of information as it applies to the UTACC system. First the CNSSI 4009 defines information as a “representation of knowledge such as facts, data, or opinions in any medium” [6]. Naval Doctrine Publication (NDP) 6 states “information is the raw material of decision making and execution” [1]. Although the definitions from these two sources differ, they both highlight information as a key component to knowledge and ultimately the ability to make decisions. As seen in Figure 1 from NDP 6, information is derived from data, translated into information, analyzed or fused into knowledge, which ultimately leads to an understanding [1].

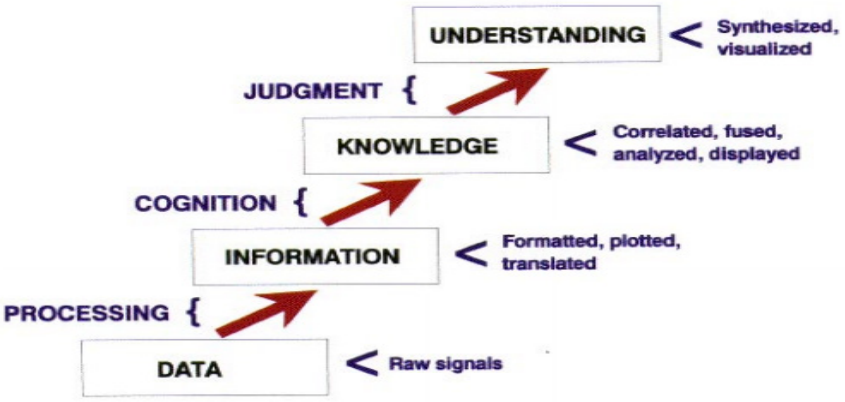

Figure 1. The Cognitive Hierarchy, from [4], shows how raw data is processed into understanding.

"Assurance" is the second portion of the term "information assurance" that must be clearly defined and analyzed. "Assurance," in the context of information systems, was defined by the National Institute of Standards and Technology (NIST) as the "degree of confidence that the security controls operate correctly and protect the system as intended" [9]. To obtain assurance an accrediting official makes the final decision about how much and what types of assurance are needed for a system and this official is the arbiter of assurance [9]. To have "assurance" in an information system, by definition the system must be protected via security controls and someone must accept responsibility for the system and the inherent risks of the system.

1. The Five Pillars of IA

The CNSSI 4009 lists five characteristics of IA: *availability*, *integrity*, *authentication*, *confidentiality*, and *non-repudiation* [6]. These five concepts are also included in the DOD directive 8500.01E, which directs them to be included on the design and operation of a secure information system [10]. To best employ these concepts they must be fully understood as they relate to the information system and the environment the information system is going to be employed. Confidentiality, integrity, and availability are commonly known as the CIA triad [11]. Focusing only in the CIA triad, NIST issued Federal Information Processing Standards (FIPS) Publication 199 for the purpose of

creating and maintaining guidelines for the examination of an information system [12]. DOD uses the additional two concepts of *non-repudiation* and *authentication* when they analyze a system. As UTACC will be a DOD information system, this chapter will explain the five pillars of IA.

a. Availability

The concept of availability is relatively simple when compared to the other four. The Title 44 legal definition is ensuring the "timely and reliable access to data and information services for authorized users" [7]. Including the word "authorized" into the definition is what makes this concept a piece of the overarching IA structure. Without this term the concept is simply defining network access. The CNSSI definition includes the concept of usability [6], which brings up an interesting and sometimes clashing idea to IA being simple. DOD still uses the 2002 CNSSI definition for availability [10].

b. Confidentiality

CNSSI 4009 states confidentiality is "the property that information is not disclosed to system entities ... unless they have been authorized to access the information" [6]. An information system is said to have confidentiality if it can deny access to its organic information to unauthorized individuals or other systems. According to DOD Directive 8500.01E the DOD is still using an older definition of confidentially which is simpler than the CNSSI 4009 one [10]. Some academic definitions include in the concept of privacy within the definition of confidentiality. This definition includes the process by which individual systems collect and disseminate information [11]. Due to the scope of this thesis privacy will also be discussed.

FIPS 199 has a differing definition for confidentiality, and because of its importance to the standardization process for system's security for NIST that definition should also be discussed. The NIST definition is taken from U.S. law [12], which states, "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information" [7]. This is the legal definition and is where the usage of the CIA triad by NIST can be traced. This definition points at the means of providing protection and not the overall aims or desired goals. The

importance of unauthorized use and access are visible here as well as the importance of privacy.

c. Integrity

U.S. law defines integrity as "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity" [7]. The difference between this definition and the one from the CNSSI 4009 is that it does not include or focus on the system itself. CNSSI 4009 includes, "an entity has not been modified in an unauthorized manner" [6]. This focus on the system is what breaks this definition out from the previous one. The use of both of these definitions can lead to confusion of what is actually being protected, the information or the system. According to academic definitions system integrity and data integrity are both equally important [11]. The DOD definition focuses on the hardware and software of a system as well as the integrity of the information [10].

Returning to the legal definition it is seen that non-repudiation and authenticity are legally included under integrity [7]. This explains why many only focus on the CIA triad and not these two topics individually. DOD has separated these two topics though and considers them equally important to the original three pillars of the CIA triad [10].

d. Authentication

According to U.S. law, authentication falls under integrity [7], but because of the importance placed on authentication by DOD it will be discussed at the same level as the rest of the CIA triad [10]. Although it is broken up as its own topic within DOD it does not have a legal definition. CNSSI 4009, the IA dictionary, defines authentication as "the process of verifying the identity or other attributes claimed by or assumed of an entity, or to verify the source and integrity of data" [6]. Verifying the source of the data is known as data provenance [13]. The DOD definition does not include a discussion on data provenance, but instead it emphasizes confirming a user's authorization and the legitimacy of the message [10]. Academic discussions on authentication also include the idea of data provenance. This means that while overlooked in the definition from DOD,

the concept of verifying the source of the data is important to the analysis of an information system especially for a system like UTACC.

e. Non-repudiation

Again, like authentication, non-repudiation legally falls under integrity [7]. DOD breaks it apart though and believes it equal to the other concepts within the CIA triad [10]. DOD refers to the CNSSI 4009 definition where non-repudiation is defined as " the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information" [10]. This provided accountability significantly increases the ability to investigate or analyze in the case of a security breach [11]. The concept of verifying orders and authority is well understood within the DOD construct and it is obvious why this is of great importance.

2. Risk Management

As with any system in today's information environment, especially within the area of defense, there is an inherent risk involved with operations. How can risk be identified and avoided or mitigated? CNSSI 4009 defines risk as a

> Measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence. [6]

That said a low-risk event would be one that has either a minimal impact, or an unlikelihood of occurrence. High-risk events would be either ones with high likelihood of occurrence, or significant impact. The process of identifying risks, conducting a risk assessment, implementing a risk mitigation strategy, monitoring the security state, and documentation of said process is known as risk management [6]. NIST SP 800–39 was developed by NIST to define how organizations deal with risk [14]. A major tool used for this is the Risk Management Framework (RMF).

a. Risk Management Framework Background

NIST's RMF is a tool used to analyze an information system to discover its weaknesses and required security controls. When conducting a risk assessment NIST SP 800–30 states the RMF should be used [15]. NIST SP 800–53 [16] introduces and explains the RMF process. For consistency within Federal Information Systems RMF was developed alongside the DOD and other U.S. Government agencies [17]. NIST SP 800–37 encompasses details on how RMF is used for Federal Information Systems [17]. According to this guideline RMF is only applicable to Federal Information Systems and not national security systems [17]. Due to UTACC's usage and managing of intelligence it is classified as a national security system under Title 44 U.S. Code [7]. Regardless, the RMF process offers tools that can be useful in evaluating UTACC.

b. RMF Steps

Figure 2 shows the six steps of the RMF process. The steps of the RMF process approach responding to risk in a fluid fashion and enable quick response in a changing environment [17].

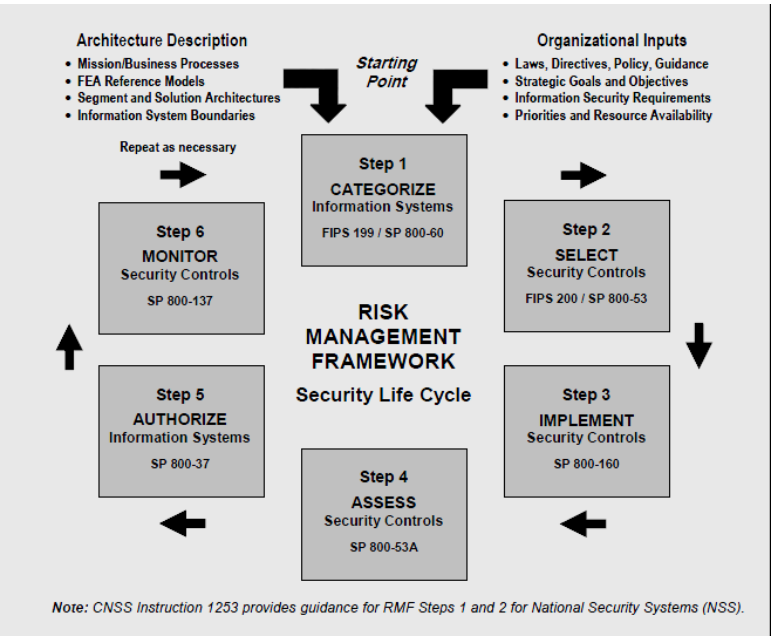

Figure 2. Risk Management Framework, from [16], shows the steps taken in the risk management process.

(1) Categorize Information Systems

The first step conducts impact assessment using FIPS 199 [12]. This assessment depicts the impact of events on the mission of an organization if said events are allowed to occur. It assigns a score to each threat (high, moderate, low, or not applicable) based on the impact of the threat to the mission of the organization. It uses the three elements of the CIA triad to establish the outcomes of risks if in-place security controls should fail. Each risk is then assigned a security categorization based on the impact assessment results. The potential impact to the system is determined based on vulnerability assessment and the analysis' understanding of the threat's capability [12]. Since UTACC is a national security system, by the legal definition [7], this exact process cannot apply, but the steps of conducting an analysis and determining security controls is still important to understand.

(2) Select Security Controls

This step takes the output of the previous step, the categorization, and assigns applicable security controls [17]. The score from the assessment of each of the CIA triad's elements is used when assigning security controls. FIPS 200 [18] lists the seventeen possible security related areas that security controls are split into. NIST SP 800–53 [16] defines the security controls and provides guidance on adapting controls to suit the vulnerability.

(3) Implement Security Controls

This step takes the output from the previous step, the security controls, and inserts them into the information system. Ideally, a new system such as UTACC, considers the required security controls prior to developing the system. Documenting and tracking changes is key to this step as changes to the information systems will need to able to be audited later [16].

(4) Assess the Security Control

As the security controls are implemented this step will conduct an assessment of the implementation to ensure the desired outcome is achieved. Suitable procedures are used in the assessment to ensure the intended effect is attained [17].

(5) Authorize Information System

This step is more of a sanity check for the information system's owner. During this step the owner will determine if the risks after implementing controls are acceptable for operation [17]. If the system is considered acceptable, the system is approved for operation.

(6) Monitor Security Controls

As with any process the maintenance of the effect is important. This step encompasses the constant reevaluation of the information system to ensure the consistent effectiveness of the implemented controls. If changes are required, appropriate channels are used to make changes to the controls to increase the effectiveness of the information system [17]. This step ends when the information system is no longer in use.

3. Security Classification of National Security Systems

As stated above, the classification of UTACC as a national security system does not allow the RMF process to be utilized [17]. Because of this CNSS developed its own instruction for national security systems, which is found in CNSSI 1253 [19]. This establishes the method of conducting the security classification of national security systems [19]. Similar to RMF, CNSSI 1253 uses those classifications to establish security controls.

a. Classification Method

An impact of low, moderate, or high is established for each risk through the lens of each of the CIA triad attributes. This is very similar to the FIPS 199 process. High impact risks are those with a disastrous adverse effect, which in turn could mean mission critical failure, substantial damage to assets, or significant harm to personnel [19]. A moderate risk impact has serious affects to mission success, harm to assets, and possible harm to individuals [19]. A low risk impact would have a limited affect to personnel, assets, or the mission [19].

The above classifications are based on the worst case assessment of impact including all factors that can affect the CIA triad, though they are evaluated separately

from each other [19]. One major difference between this classification method and the FIPS 199 is that no national security system can rate lower than moderate in the confidentiality category [19]. The classification of the information the systems handle is the basis for this rule, which is valid as the data itself has a significant role in the very nature of the mission. There are additional concerns for confidentiality within UTACC due to the information sharing between users and systems in its processes, and the aggregation of data within certain vehicles.

b. Security Controls

Similar to the RMF the next step in the CNSS method, once classification is complete, is to assign security controls. This is done in a four-step process. The first step is to assign a set of controls based on the classification using a table in the CNSSI 1253 [19]. Next, the security control overlay is selected and applied to the risk. Third, the security controls are tailed to fit into the information systems for which they are needed. Last, the new controls are augmented with each other. It is important to acknowledge that all the controls available will never be able to fully eliminate all risk to the information system and the data within [19].

4. DOD Information Assurance Certification and Accreditation Process (DIACAP)

The Defense Information Assurance Certification and Accreditation Program is a policy in which the DOD shall certify and accredit information systems through a process for identifying, implementing, and managing IA capabilities and services [20]. It is essential to view any system, including UTACC, which processes, stores, and disseminates information across the battle space utilizing this process. This process evaluates defense in depth levels of IA risk reduction that applies to personnel, hardware, software and processes and ensure appropriate protection of these assets [20]. Defense in depth is a key strategy in network security, which reduces an attack vector on a vulnerability of a system by introducing security controls. Currently UTACC is a demonstration system only and the regulations surrounding the DIACAP process do not apply due to it not connecting to a live DOD data network. However, The DIACAP

process provides the framework that the authors will follow to evaluate the UTACC system.

> This handbook establishes a standard process to identify, implement, and validate standardize Information Assurance Controls (IAC), authorizing the operation of the Department of the Navy (DON) information systems (IS), and managing the IA posture for the duration throughout the DON's IS's life cycle. [20]

The handbook also develops procedures for information assurance controls, including their identification, implementation, and validation [20]. To further describe the scope, purpose and importance of IAC's.

> IACs are employed in such a manner that information and resources are provided with the appropriate level of security commensurate with mission criticality, level of effort, and classification or sensitivity level of information received, processed, stored, displayed or transmitted. [20]

Information systems such as UTACC will be used for collecting, displaying, storing, transmitting, and receiving data or information that will be classified or sensitive in nature. One concern that should be addressed is deciding the classification level that UTACC should use to provide security for the system [21].

The DIACAP utilizes five distinct phases in order to complete the process: Initiate and Plan Information Assurance certification and accreditation (C&A), Implement and Validate Assigned Information Assurance Controls, Make Certification Determination & Accreditation Decision, Maintain Authority to Operate and Conduct Reviews, and Decommission. [20]. To completely understand the process and how it will impact the UTACC system a more detailed review of these five phases will be required.

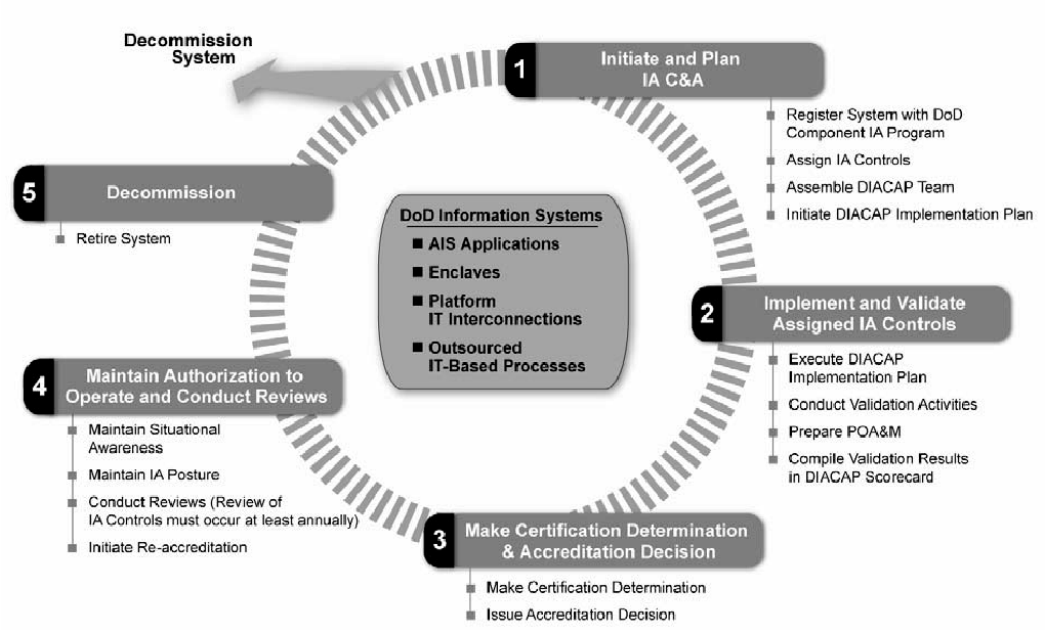

Figure 3. DIACAP Process Flow Chart, from [3]

B. THE CYBER SECURITY MATRIX

The purpose of our analysis of the UTACC system is to achieve IA. In this chapter the pillars of the CIA triad are matched against the concepts of threats, vulnerabilities, and security controls. To completely examine the UTACC system we look through the lens of the three main surface areas in which threats exist. These areas are people, technology, and operations. The nation's people, technology, and operational experience provide the DOD with a strong foundation on which to build its military and civilian workforce and advance its technological capabilities [22]. Even though these surface areas present a strength, they also are an avenue to mount threats and exploit vulnerabilities. To combat these threats, security controls must be established or preplanned to mitigate vulnerabilities. Each of the three areas are equally important in evaluating an information system such as UTACC. Figure 4, the cyber security matrix, is a tool comprised of each of these terms, and will be used to perform threat and vulnerability assessment of the UTACC system. The assessment will also include the recommendation of security controls through the concept of defense in depth.

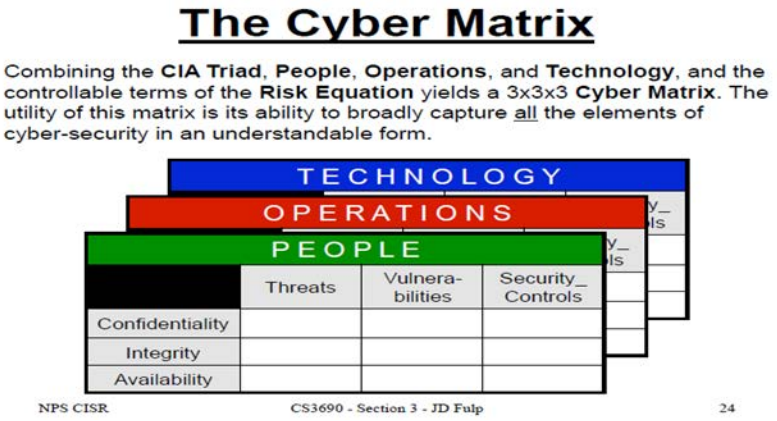

Figure 4. The Cyber Matrix, from [23], shows the basic relationship between the CIA triad and threats, vulnerabilities, and security controls as they apply to people, technology, and operations.

1. People

People are an integral part of UTACC system development, will perform command and control functions of the UTACC system, and will utilize the information processed by the system. Therefore, "people" must be a part of the threat and vulnerability assessment. A key component to effective command and control is people [1]. Command and control are essential in regards to the employment of an unmanned or autonomous information system, like the UTACC. People, as an element of command and control, gather information, make decisions, take action, communicate, and cooperate with one another in the accomplishment of a common goal [24].

The same people that make information and information systems effective are also an important part in achieving IA, which is also part of the overall goal. People are the Department's first line of defense in sustaining good cyber hygiene and reducing insider threats [22]. People play a major role in the defense in depth strategy by creating policies and procedures, training and awareness, system security administration, physical security, personnel security, and facilities countermeasures [8].

The people present a vulnerability for exploitation via information and information systems. People have been exposed as a weakness to IA and exacerbate threats to information and systems. Achieving information assurance with people must be

coupled with policies and procedures, assignment of responsibilities, commitment of resources, training of personnel, and through personal accountability [8]. The CSI Computer Crime and Security survey indicated that 43.2 percent of respondents stated that at least some of their losses were attributable to malicious insiders (people), and 16.1 percent of respondents estimating that nearly all their losses were due to non-malicious people [25]. To mitigate the threats inherent in the people in the cyber security matrix the DOD has set the following guidelines.

> DOD seeks to foster a stronger culture of information assurance within its workforce to assure individual responsibility and deter malicious insiders by shaping behaviors and attitudes through the imposition of higher costs for malicious activity. This cultural shift will be enabled by new policies, new methods of personnel training, and innovative workforce communications. [22]

2. Technology

This section will clarify the intersection between the UTACC system and technology, while exposing technology as a threat to achieving IA. Although the UTACC system's specific technology is irrelevant and agnostic at this point in the UTACC system development, the ability to identify certain technology-related shortfalls is paramount in understanding how to procure, protect, and operate the UTACC system. The very technologies that empower us to lead and create also empower those who would disrupt and destroy [22]. Technology is defined as the "application of scientific knowledge for practical purposes" [26]. The application of technology enables the UTACC system to operate effectively. Pairing the terms "information" and "technology" together is the basis for the UTACC system.

Information technology is the use of "systems to store, send, and retrieve information" [27]. The UTACC system will conduct these tasks to ensure effective collaboration internally between system components and externally with Marines. The information that is in these different states (stored, in-transit) is what must be protected. The Statement of Work (SOW) states that the UTACC system will conduct intelligence, surveillance, and reconnaissance (ISR) missions and with some level of autonomy [28].

The task of developing an autonomous system to complete ISR missions is daunting, but current related technologies are being employed by all departments in the DOD.

The DOD's depth of knowledge of information and communications technology, paired with its cybersecurity expertise, provides the Department with strategic advantages in cyberspace [22]. The DOD may have an advantage, but technology in a system such as UTACC provides an avenue for a wide range of threats. One example of a technological threat is that software and hardware technology are at risk of malicious tampering even before they are integrated into an operational system [22]. This technological threat is not aimed specifically at the UTACC system, but must be addressed before the system is procured. The majority of information technology products used in the United States are manufactured overseas and the dependence on technology from untrusted sources diminishes the predictability and assurance that DOD requires [22]. A technologically advanced system, like the UTACC system, could become susceptible to this threat. Although the technology has not been fully researched, developed, or tested, the threats against similar and emerging technologies are present and must be analyzed.

3. Operations

The UTACC system should be developed to conduct expeditionary operations across the full range of military operations in any environment. The UTACC system will be expected to conduct missions in any environment to collect, process, analyze, and exchange information rapidly in support of operations planning and execution [29]. The operations area reflects on daily operations that make up the security posture for the organization [8]. These daily operations are unique in regards to the UTACC system. The UTACC system will be required to operationally integrate with air and ground elements of the MAGTF. This will include any organizational routines, procedures, or protocols that are currently in place to foster a secure and safe environment.

The UTACC system concept of operations is being developed by another team of Marines at the Naval Postgraduate School. Team One provides the foundation for the operational employment of the UTACC system. Many factors will determine the operational impacts of the UTACC system, but the following are the tools required to

ensure that threats to the UTACC system are mitigated to an acceptable level. The NSA lists the following guidelines for sustaining the security posture of an organization.

> 1. Maintaining visible and up to date system security policy. 2. Certifying and accrediting changes to the Information Technology baseline 3. The C&A processes should provide data to support "Risk Management" based decisions. 4. Managing the security posture of the Information Assurance technology (e.g., installing security patches and virus updates, maintaining access control lists).5. Providing key management services and protecting this lucrative infrastructure. 6. Performing system security assessments 7. Attack sensing, warning, and response. 8. Recovery and reconstitution. [8]

These steps are baseline controls to mitigate the risk against UTACC system operations. All of these steps are critical in regard to the employment and operation of the UTACC system. The operation and employment of air and ground autonomous or semi-autonomous systems will incur more operational risks that are very different from non-autonomous computer systems.

Autonomous systems represent a new class of devices whose security requirements appear to differ greatly from those of conventional computer and computer networking systems [21]. The system and the unit employing the system must have the following four steps provide assurances for how to control physical access to the system, which is operational in context (1) "There must be an explicit and well-defined security policy enforced by the system;" (2) "Access control labels must be associated with objects;" (3) "Individual subjects must be identified;" (4) "Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party" [21]. Understanding the entire operational lens (employment, integration, and environment) is critical in identifying current threats and vulnerabilities of the UTACC system.

4. Threats

The main goal of this thesis is to provide a threat assessment for the UTACC system. This assessment will require a comprehensive review of the term "threat" and how that term relates to an information system like UTACC. The term "threat" is defined as the potential for a particular threat-source to successfully take advantage of a particular

vulnerability [15]. Threats can occur from many different things and people in regards to the UTACC system. A threat-source is any circumstance or event with the potential to harm an IT system [15]. The UTACC system is unique in that the threat source area is expanded due to where and how the system will operate. People, technology, and operations will cover the entire threat spectrum. Due to the technical nature of the UTACC system, cyber threats must also be discussed. Cyber threats are defined as "the possibility of malicious attempt to damage or disrupt a computer network or system" [30]. Douglas Gage separates threats in the following manner: violations of secrecy (confidentiality), violations of data modification (integrity), and denial of service (availability) [21]. The cyber matrix accounts for all threats regardless of violation, or the avenue (people, technology, or operations) in which the threat will originate. The UTACC system will not be at risk from a threat-source if it does not have vulnerabilities to be exploited.

5. Vulnerabilities

The term "vulnerability" is also a key term to understand in relation to the UTACC system. Vulnerability is defined as a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source" [15]. These flaws or weaknesses create gaps that can be exploited accidentally or intentionally by anyone who has access to the system.

A vulnerability assessment of the UTACC system will be extremely difficult because the system has not yet been designed. The NIST SP 800–30 states that if the "IT system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendors' or developers' security product analyses (e.g., white papers)" [31]. The security policies and planned security procedures of the Marine Corps, paired with an assessment of vulnerabilities in current IT and unmanned systems will be researched to provide a foundation for system designers and developers to consider.

6. Security Controls and Defense in Depth

"Security controls" is another term that must be analyzed as it is a major element in the assessment of the UTACC system. Security controls are defined by NIST SP 800–30 "as the safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information" [15]. "Security controls encompass the use of both technical and nontechnical methods" [31]. These different methods will enable the UTACC system to effectively mitigate vulnerabilities that are either technical or nontechnical in nature.

"Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software)" [31]. The UTACC system will have to employ technical security controls due to the highly technical nature of the system referenced in the Statement of Work (SOW) [28]. "Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security" [31]. These non-technical controls will encompass all other controls required to ensure UTACC system integration through policies and procedures in the operational environment.

Each of these methods (technical and non-technical) have sub-categories (preventative and detective) that must be explained to ensure the types of security controls being employed. "Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication" [15]. "Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums" [15]. Security controls are a means to mitigate vulnerabilities to an acceptable level of risk, which allows for a person to assume responsibility for any information system, including UTACC

A best common practice for achieving information assurance is the use of redundant security controls in a defensive plan. This practice is known as the Defense in

Depth concept [8]. The DOD definition explains how to achieve IA through defense in depth:

> The DOD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness. [10]

The mitigation techniques (protective mechanism) are layered throughout the entire threat surface area. This concept of layering (rings), redundancy, and separate lines of defense is visible in Figure 5.

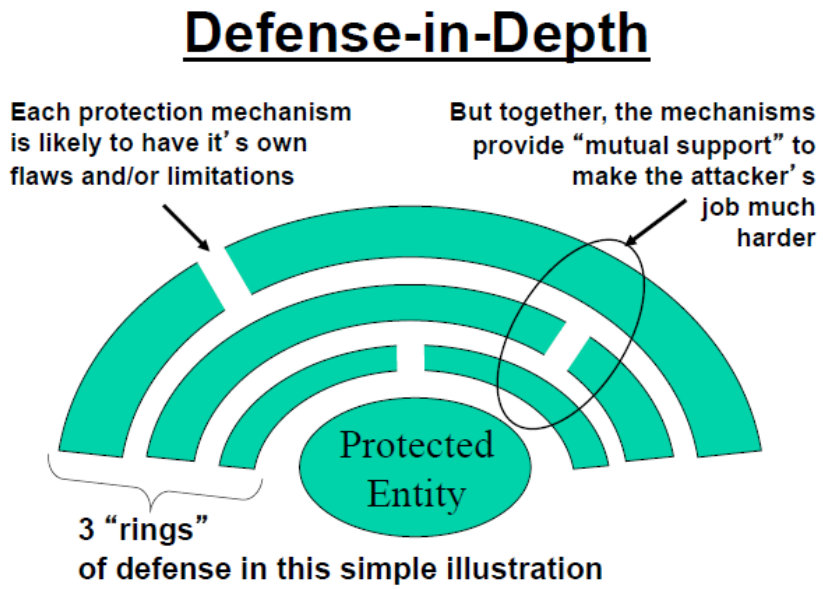

Figure 5. Defense-in-Depth, from [23], depicts how gaps in certain lines of defense are supported by other forms of defense.

As a demonstration system only, many of the concepts and principles above will not apply due to the system never being employed on a live DOD data network or on a battlefield. The next chapters apply the concepts above to a theoretical UTACC system that would be both connected to a DOD data network and employed on a battlefield alongside the Marines.

III. METHODOLOGY OF ANALYSIS

This chapter will explain the creation of the threat template which was designed to assess the UTACC system by identifying security shortfalls. Second, the chapter will explain each individual section of the threat template. This template will include all the elements from the Cyber Matrix, the threat selection process, system impacts, and the projected effectiveness of security controls. The use of this template will enable mission critical weaknesses to be discovered. The weaknesses will need to be addressed prior to UTACC system development.

A. TEMPLATE CREATION

Due to the plethora of threats the UTACC system will be exposed to, the authors decided to simplify the process of explaining and assessing each threat. To streamline the analysis, cover the maximum number of threats, and increase the utility of this thesis the threat template was created. This template allows for the individual assessment and understanding of specific threats that could impact the UTACC system, without confusing the reader in the process. Due to the diverse audience the authors attempt to bridge the language barrier between Marines and technical designers and developers.

The authors included all the cyber security matrix elements in the threat template as a baseline to evaluate the UTACC system as an information system. Additionally, the authors added assumptions to assist system developers to understand the environment the UTACC system will operate within. System impacts were added to depict the gravity of each threat to the team and system if not mitigated. The impact of security controls relates the impacts of mitigation strategies to the design, fielding processes, and costs of the UTACC system.

The NIST's guide for conducting risk assessments served as an influence to the template creation process. Specifically, publication 800–30 shows a model (Figure 6) that assisted in the design of the threat template. Many of the concepts therein, such as likelihood of threat success, degrees of impact, and organizational and operational risk can be seen mirrored in the threat template designed for this thesis [15].

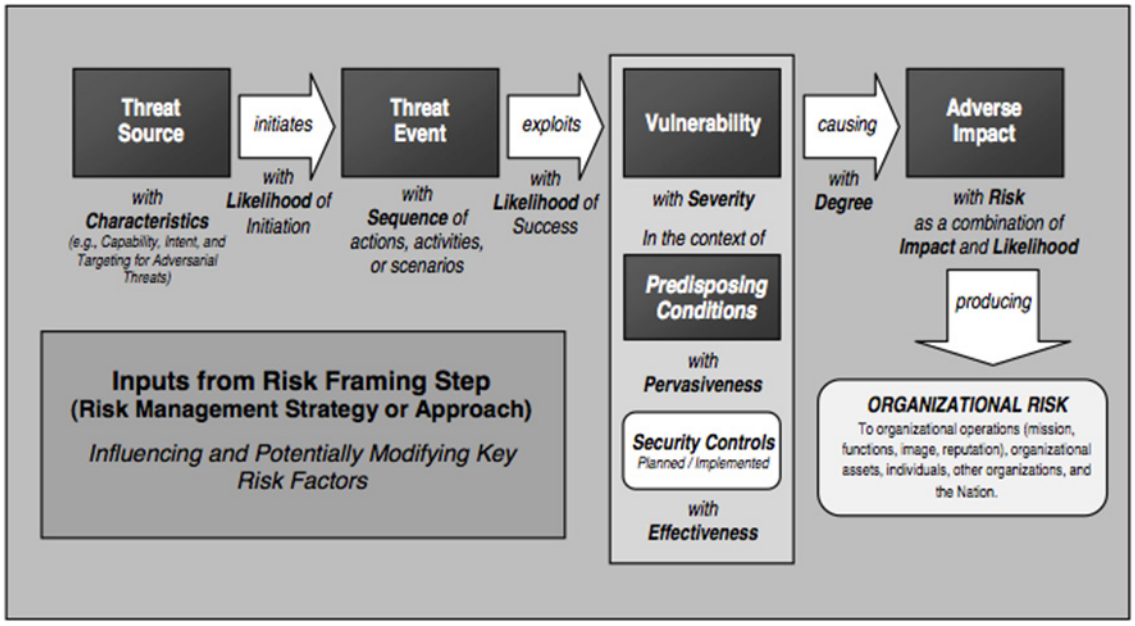

Figure 6. Generic Risk Model with Key Risk Factors, from [15], shows how risk is defined from a threat source.

B. BREAKDOWN OF THREAT TEMPLATE

The diversity of threats that exist against an information system requires a study of each piece of the vast threat surface area of the UTACC system. Figure 7 shows the template used to research each threat and the components of each threat.

UTACC THREAT ANALYSIS WORKSHEET

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	THREAT
THREAT SUMMARY	
IMPACT TO THE CIA TRIAD	
IMPACTS TO UTACC	
VULNERABILITY ANALYSIS	
ASSUMPTIONS	
SECURITY CONTROLS	

Figure 7. Threat template shows the sections included in the template used for each threat assessment.

1. Threat Area

The list of threats is selected from the threat areas of people, technology, and operations. Threats exist that span separate areas, and threats exist that are either technologically or operationally based, or both. The cyber matrix discussed in Chapter Two serves as a guideline for sorting through threats and deriving the area in which the threat exists. To classify each threat within a specific threat area questions regarding the threat's target or specific vulnerability were asked. This can be separate from what is actually affected by the threat itself. For example a phishing attack is an attack against the threat area people, but the effects of the attack can be seen in technology and operations. Many threats exist within the scope of just one threat area, but some span two or more areas. An example of this is the ownership / maintenance of the UTACC system where the threat area spans both people and operations.

2. Threat Selection Process

The threat list generated is in no way comprehensive, but allows for the research to delve into the range of both the simple and complex threats needed to aid in the design and development of the UTACC system. It would be impossible for this thesis to conduct an in-depth analysis of every threat that may exist against the UTACC system. The authors also attempted to get an even spread of threats affecting people, technology, and operations. The discussion will account for the reality that the UTACC system will be operated in a kinetic environment, which introduces some unique threats that must be thought through prior to system design.

3. Threat Summary

The threat summary section includes many parts and is the largest section of the template. This section serves as the core of the template, while at the same time fulfilling a flexible catchall function. The purpose of this section is to explain the threat itself in detail. Included are any relevant background information or history, the threat's definition, and how the threat itself would apply to the UTACC system specifically. Information from the authors' experiences throughout their time in the USMC is included if relevant to the information being presented. Lastly, both the most dangerous and most likely results of the threat are presented along with an example of each. These results explain the impact of the threat to the system, team, and the mission.

4. Impact to the CIA Triad

This section names the pillar or pillars of the CIA triad that are affected by this threat. The CIA triad, from Chapter Two, consists of confidentiality, integrity, and availability, each of which affects the UTACC system's ability to operate very differently. The triad allows the research to assess each threat from the standpoint of how the information is affected by the threat. The access of information by unauthorized individuals compromises the confidentiality of the UTACC's information. Modification or destruction of information compromises the integrity of UTACC's information. Denying access to the information compromises the availability of UTACC's

information. A threat may not necessarily target just one pillar of the triad, but can target two or all three in different or unique ways.

5. Vulnerability Analysis

To completely understand where in the UTACC's life cycle a threat exists, the template includes a section on vulnerability analysis. This section identifies the point or period during which a vulnerability appears against the UTACC system. As each point of vulnerability is different, they may require unique security controls to be put in place at various times throughout the UTACC system's development and operation. The threat arises during a specific point or period; however, security controls can be put in place at any time. The range of vulnerable times includes initial research and development, manufacturing, fielding/training, and finally during any operation or maintenance phase.

6. Assumptions

Certain assumptions were made throughout the threat selection and analysis process. These assumptions were made based on USMC doctrine, technology, the operating environment of the UTACC system, and the authors' experiences. The assumptions based on doctrine are those that account for tactics, techniques and procedures (TTPs), standard operating procedures (SOPs), the maintenance cycles, and staff planner's timelines. Assumptions on technology include those regarding the current state of technology as well as the future technology that may exist at the time of UTACC fielding and operation. Assumptions on the operating environment of UTACC include enemy capabilities ranging from those encountered in our recent campaigns in Iraq and Afghanistan to enemy capabilities of near-peer countries as well as factors such as weather and terrain. The assumptions based on the authors' experiences in the Fleet Marine Forces are those that account for the nature of Marines and unit commanders and the value that both mission accomplishment and the lives of Marines play in an operation.

7. Security Controls

Security controls are safeguards implemented to mitigate specific vulnerabilities. These security controls are recommended after analyzing where the UTACC system is

vulnerable to each threat. Security controls include technical and non-technical controls. Technical controls include system specific modifications or capabilities. Non-technical controls include training for operators, maintainers, and planners; operational and maintenance procedures; and early integration into the doctrine and policies that guide USMC operations.

IV. ANALYSIS

The purpose of this chapter is two-fold. First, a section is included which further classifies each threat into threat types beyond the broad areas of people, technology, and operations. This classification is designed to assist the reader in navigating through the appendices. Second, this chapter will explain one threat using the template presented in Chapter 3. The discussion of how the template was used to frame this threat will enable the reader to easily process the additional 28 threats to the UTACC system.

A. THREAT TYPE CLASSIFICATION

All twenty-nine threats are provided in the appendices. These templates are designed to be both an integral part of the thesis as well as stand-alone documents. Because of this, the reader will encounter repetition of often repeated security controls. For organizational purposes the threat templates were organized by the threat areas of people, technology, and operations.

The threats analyzed within the people threat area include Insider Threat and Phishing which are grouped together because they deal with a rogue actor. Ownership and Maintenance of UTACC, Attitude Towards Emerging Technologies and Equipment, and Autonomy as an Ethical Concern are the remaining people threats which are grouped together because they deal with people that do not necessarily have a malicious intent.

The threats analyzed within the technology threat area are broken down further into (1) Threats with a malicious actor, (2) Threats that arise within the UTACC's operational organization, and (3) The technology of UTACC itself. Threats with a malicious actor include Spyware, Jamming of C2 and Data Links, Denial of Service Attack, Eavesdropping, An Attack on Mobile Devices on a Wireless Network, A Computer Virus Targeting the UTACC system, Impersonation or Spoofing of a UGV or a UAV, and Spoofing an IP or MAC Address of a UTACC System Component. The threats that arise from within the UTACC's operational organization include Unprotected Information Stored on the UTACC System, Frequency Management and De-confliction, and UTACC System Integration with Legacy and Newly Procured Systems. The last

threat area applies directly to the technology of UTACC and includes Autonomous Software, Unencrypted C2 and Data Links, and Controlled Cryptographic Item Employment Onboard an Autonomous System.

The threats analyzed within the operations threat area include threats to the design and integration of the UTACC system and threats against the employment of UTACC. Threats to the design and integration of UTACC include Cost Threat to UTACC System Research, Development, and Testing; Airspace Integration; Surface Space Integration of UTACC; and Human Machine Interaction. Threats against the employment of UTACC include Reconnaissance Team Employment of UTACC, Survivability of the UTACC System from Enemy Weaponry, Environmental Threats, Terrain, Shipboard Operations, and Operational Endurance.

B. AIRSPACE INTEGRATION

The authors chose the threat of Air Space Integration (Appendix U). Airspace Integration was chosen to illustrate the dynamics of not only viewing the UTACC system as an information system, but also as an asset within the Marine Air Ground Task Force (MAGTF). As such, the example threat serves as a bridge between a typical information system and the unique capabilities of the UTACC system.

1. Threat Area / Threat

As outlined in the Statement of Work, "UTACC shall consist of both a ground component(s) and an aerial component(s) acting in a collaborative fashion as a single system with a single operator" [28]. This threat exists in the operational threat area because it has the potential to affect UTACC system operations. This threat affects the airspace system and all actions that take place in this domain. The introduction of a semi-autonomous aerial vehicle into the airspace system increases the risk to military operations in this domain. This can be seen in Figure 8.

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	THREAT
Operations	Airspace Integration

Figure 8. Threat Area / Threat depicts the categories this into which this threat template falls.

2. Threat Summary

The threat summary (Figure 9) for the Airspace Integration threat links the current operational environment with the specific threat to the UTACC system. Due to the specification of Airspace Integration this section includes relevant recent history within DOD, current USMC employment of similar systems, where UTACC fits in this threat environment, and the most dangerous and most likely outcomes of this threat. The flexibility of this section allows for threat-specific information such as experience, relevance, and gravity of the threat to be included when needed.

THREAT SUMMARY

The procurement and utilization of unmanned systems has increased significantly in recent years. The U.S. had fewer than 10 Predator Unmanned Aerial Vehicles (UAV) in 2001 and the fleet grew to 180 by 2007 [57]. Predator UAVs carried out 2,073 missions from June 2005 until June 2006 [57]. Manned and unmanned aircraft are already taking a large share of the airspace system. UAVs operate either autonomously via onboard computers or sensors or semi-autonomously (with a human in the loop). Fully and semi-autonomous unmanned aerial vehicles have the capability to operate at the same altitudes as manned aviation assets. The seamless integration of UTACC into an already crowded airspace system must occur before UTACC is ever employed in a real world scenario.

Development of UTACC will require an in-depth study of current policies, procedures, and regulations that govern both the military and civilian utilization of the airspace system. The USMC currently utilizes three different types of UAVs. Larger UAVs like the Shadow and STUAS require adherence to the Naval Aviation Training and Operating Procedure Standardization (NATOPS) and must be operated by trained Aerial Vehicle Operators (AVO) and Mission Commanders (MC) who are integrated into the Air Command Element (ACE). Both the Shadow and Small Tactical Unmanned Aerial System (STUAS) UAVs are classified as Group Three UAVs. The Shadow UAV operates between 4,000 and 10,000 feet Above Ground Level (AGL), while the STUAS UAV operates between 1,500 to 5,000 feet AGL [38]. Both the Shadow and STUAS will appear on the Air Tasking Order (ATO) with the operating times and altitude to integrate into the airspace with manned aviation assets [38]. The Shadow and STUAS UAVs are equipped with a transponder enabling positive and procedural control, which requires two way communication with the controlling agency (DASC/FAC) [38]. The smallest UAV operated by the Marine Corps is the Raven which may be a comparable size to the UTACC UAV. Raven UAVs operate at or below 1,200 feet AGL, which is coordinated by the battalion air officer to integrate with rotary wing assets and they do not require a trained MC or AVO to operate [38]. A detailed review of how current UAVs are employed by the Marine Corps will provide the foundation for integration of UTACC. As the UTACC design solidifies and as requirements increase, the size of the UAV will determine who and how the system will be employed. A completely autonomous air vehicle operating in congested airspace above a target or area of interest increases the risk of employing the UTACC system.

The most dangerous variation of this threat would be UTACC being employed in support of a mission along with manned aviation assets. The UAV may be launched, without the knowledge of the aviators and a mid-air collision causes a mishap and destroys the aircraft and possibly kills the crew.

The most likely threat permutation would be the UTACC UAV being grounded due to safety of flight concerns with manned aviation assets. A reconnaissance team does not possess the resident expertise in airspace integration and will not employ the system if it endangers other airborne assets also supporting their mission.

Figure 9. Threat Summary describes the pertinent information for the threat of Airspace Integration.

3. Impact to the CIA Triad

Of the three pillars of the CIA Triad (confidentiality, integrity, and availability) only availability was impacted by the threat of Airspace Integration. Availability in this context is referring to the accessibility of the UTACC system to be utilized during an operation. Availability was deemed to be at risk because of safety of flight concerns for

the UTACC system if the security controls are not met. This would result in the UAV being grounded due to inadequate integration. This is depicted in Figure 10.

IMPACT TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

Figure 10. Impact to the CIA Triad names the area of the CIA triad that is impacted by the threat.

4. Vulnerability Analysis

The threat of Airspace Integration arises at the point when the UAV portion of the UTACC system enters the airspace system and lasts for the duration of the UAV flight, as seen in Figure 11. This point is when the specific threat has the potential to negatively impact the UTACC system or the UTACC's mission.

VULNERABILITY ANALYSIS

- When the UAV portion of the UTACC system is employed in the airspace system.

Figure 11. Vulnerability Analysis defines the point at which the threat arises against the UTACC system.

5. Assumptions

The assumptions in this threat template are provided to limit the scope of the threat analysis in the template. The assumptions for Airspace Integration focuses the reader on the importance of rules and regulations within airspace integration. These assumptions are depicted in Figure 12.

ASSUMPTIONS

- Federal Aviation Administration, Department of Defense, and specifically the reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The UAV portion of the UTACC system will be grounded if integration is not achieved.

Figure 12. Assumptions lists the relevant assumptions for this threat.

6. Security Controls

The non-technical security controls were chosen to ensure system designers and decision makers understand two key things not related to the physical aspect of the system. First, they must understand the importance of the governing regulations of the airspace system which enable proper integration of the UTACC system in this domain. Secondly, they must understand the importance of training and coordination prior to the utilization of the UTACC system within the airspace system.

The technical security controls were chosen to ensure safety of flight through technological components. These controls can set limits to the autonomy or apply technical controls within the UTACC system during its operations within the airspace system. Technical security controls ensure the UTACC system has the capabilities it needs to integrate into the airspace system. Both types (non-technical and technical) of security controls can be seen in Figure 13.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future FAA, DoD, and USMC policies, procedures and publications to determine specific system requirements of the UAV. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the UAV.
  - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
  - Ensure integration within the airspace system in both a deployed and non-deployed environment.
- Technical Controls
  - Limit altitude and range of the UAV.
  - Identify UAV size and the equipment required (Identify Friend or Foe).
  - Employ mandatory semi-autonomous modes of operation.
  - Implement Independent UGV and UAV operations.
  - Ensure the UTACC mission planning component includes parameters to ensure integration with manned aviation assets and aviation command and control units.

Figure 13. Security Controls lists the non-technical and technical security controls recommended for this threat.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

This chapter presents the findings resulting from Chapter 4 and Appendices A-CC analysis. Prior to conducting analysis, the authors anticipated certain categories and patterns to arise from threats and vulnerabilities. After the research was conducted other patterns emerged that are of significant value to the ongoing analysis of information systems. Those patterns of threats and vulnerabilities found in each threat template are highlighted here. Additionally, the authors focus on the themes most commonly occurring within the security control recommendations and identify which mitigation strategies will be of the utmost importance to the development of the UTACC system.

The UTACC system is an advanced autonomous concept aimed at both information collaboration on the battlefield and at unmanned operations. However, this UTACC concept will never be a solution leveraged by the USMC without prior consideration of security and mitigation strategies, which may be applied to its inherent vulnerabilities. Creating the threat template has allowed the analysis of threats and their specific vulnerabilities. By incorporating security measures early in the design process, these threat mitigation features are integrated into the UTACC technology early on proactively. The result of not doing this early is a security policy based on reaction to threats, which means the information system is left vulnerable.

The following are answers discovered in response to the original research questions.

A. RESEARCH QUESTION 1: WHAT THREATS EXIST THAT HAVE THE POTENTIAL TO AFFECT THE UTACC?

There are many threats that exist against the UTACC system that can affect the system in many ways. They exist within the threat areas of people, technology, and operations. Some of these threats exist against the support structures for the UTACC system regardless of system implementation. As UTACC is not yet fully operational and not expected to be within the next 10–15 years, it is not possible to anticipate every threat that will exist against the system. Additional analysis is sure to find more threats as the

system matures. The existence of these threats shows the vast "surface area" for the UTACC system and proves the need to assess the vulnerabilities and apply security controls. Once UTACC is fully operational, further analysis will be required to uncover other threats. Indeed, one concept of the emerging NIST Risk Management Framework approach is to provide continuous monitoring and updating on new threats and implementing associated controls.

During the initial analysis of threats the authors saw the anticipated patterns of the people, technology, and operations threat areas. After additional research unanticipated patterns emerged. These patterns show threats existing with and without malicious actors, arising within the UTACC's operational organizations, including the technology of UTACC itself, existing against the design and integration of the UTACC system, and arising against the employment of UTACC. These new patterns, seen throughout the 29 threats, proved to be a valuable way to organize and view the threats. The addition of those threat areas to this thesis refines the broad area of threat into manageable "threat lanes" aimed specifically at the UTACC system. Those "threat lanes" will assist with the identification of additional threats to the UTACC system when the topic is researched further.

B. RESEARCH QUESTION 2: WHAT VULNERABILITIES ARE INHERENT IN THE UTACC CONCEPT?

There are many vulnerabilities within the UTACC system concept and expected employment strategy. These vulnerabilities exist within the system itself and the environment in which the system will be employed. They also exist within the employing agency, which in this case is the USMC. These patterns of vulnerability to the UTACC system were used by the authors as anticipated outcomes prior to analysis.

After conducting our analysis of vulnerabilities two distinct patterns with which to characterize vulnerabilities emerged. The first pattern categorizes vulnerabilities by the presence or absence of a malicious actor. In this pattern a malicious actor can be a kinetic (physical) or cyber (network) threat. Surprisingly, the UTACC system is vulnerable to 14 of the 29 threats without the presence of a malicious actor or enemy. This means the risk

exists within the employing organization, in the operating environment, or rests solely in the technology of UTACC. This pattern balances the threat analysis out as the remaining 15 threats do include the presence of a malicious actor.

The second pattern that emerged categorizes vulnerabilities by the point or points in the life cycle when threats emerge. As some of the threats are complex this analysis can show vulnerabilities emerging in multiple points of the life cycle. The UTACC system is most vulnerable to threats during system employment and during design or development. The UTACC system is less vulnerable to threats during fielding, demonstration, and training. This pattern will be key in determining when security controls are required for the UTACC system, and could also aid in further research in the area.

C. RESEARCH QUESTION 3: WHAT CAN BE DONE TO MITIGATE THOSE THREATS AND VULNERABILITIES WITHIN UTACC?

For each of the 29 threat templates security controls are recommended as a starting point for the mitigation of each threat. These are sorted into non-technical and technical controls. These security controls are not exhaustive, and do not consider the mitigation strategies at the component level specific to UTACC because the authors expect technology to change before system design and development.

Many reoccurring security controls can be seen in the templates in both the technical and non-technical areas. Within the non-technical category the following security controls emerged as those essential to threat mitigation.

- Policies, procedures and publications must be analyzed to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
- The UTACC system security policies and procedures must be developed to meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
- Adherence to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.

- Training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
- Extensive testing and evaluation with operational units.

Technical security control reoccurrences do not form as much of a visible pattern in the research due to the specificity of the technical security controls to the individual threats. The one security control that stands out however is the recommendation for the UTACC system to incorporate semi-autonomous modes of operation. This security control is mentioned in 27 of the 29 templates. Other technical security controls that emerged as those necessary to mitigate threats are listed below.

- Remote zeroing of software, data, and cryptographic material.
- Employ tamper resistant technology.
- Independent UGV and UAV operations.
- Redundant and encrypted C2 and data links spread across the EM spectrum.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

Those security controls included above stand out as being highly important to the UTACC system employment and must be incorporated into the design and development of UTACC to ensure success.

D. FUTURE WORK

Before the full employment of this type of autonomous system additional research that goes beyond what this thesis provides must be conducted. Continuous monitoring and analysis of newly emerging threats, vulnerabilities, and their related security controls are still required. New and emerging threats due to changing technologies may also make the security controls recommended in this thesis irrelevant. As a demonstration system UTACC is not required to go through DIACAP, but other related systems that will operate on the DOD networks will require that level of analysis. We recommend any similar system to go through a similar threat and vulnerability assessment before and after initial security controls are added.

UTACC system research is not finished. More research is required to completely analyze the plethora of threats that could not be covered in this thesis. Additionally, the

patterns of security controls emerging from this thesis require additional scrutiny. In some cases possible changes to the organizational and cultural behavior must occur prior to procuring and employing an autonomous system like UTACC. Though it is impossible to find every vulnerability, thinking about security at every stage of the design and development process will enable system designers to minimize those inherent risks.

As UTACC is not yet fully operational, it was not possible to discover and analyze every part of UTACC to find vulnerabilities. Once UTACC is fully operational, further testing will be required to uncover other vulnerabilities in the system. For this the authors recommend the further use of the threat template created during this research project. It has proven to provide utility to the analysis of the UTACC system and may continue to do so with this system and similar systems.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. INSIDER THREAT

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
People	Insider Threat

THREAT SUMMARY

An insider threat includes but is not limited to bugs, wiretaps, recording, and shoulder surfing (looking over a co-workers shoulder while they are working on a computer) [32]. These threats are prevalent in any information or unmanned system because people will inevitably operate, maintain, and manipulate the system. The federal government and the Department of Defense (DOD) have been targeted by insider threats since the founding of the country [33]. An insider threat is essentially espionage with the intent to steal, alter, destroy or degrade information or information systems. An insider threat is serious with regards to the damage a potential user can have on a system, organization, and people [34]. An insider threat affects all three attributes of the CIA triad making it a dangerous threat.

The most dangerous threat possibility would be an insider manipulating the software or the system to affect the mission outcome or to endanger personnel. An example would be a team member with access to the UTACC system modifying the specific mission software and causing the system to attack itself or the team. The Unmanned Aerial Vehicle (UAV) could be programed to crash into team members or into the ground vehicle. The Unmanned Ground Vehicle (UGV) could be programmed to run over team members.

The most likely threat impact would be a team member or contractor has access to the system and steals information, software, or mission data with the intent to distribute the stolen information to a foreign government or enemy.

IMPACTS TO THE CIA TRIAD

- An insider threat directly impacts confidentiality, but combined with other threats could impact data integrity and availability [32].

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The UTACC system will require some form of physical security to protect

cryptographic material and keys.

- Network access is a requirement for the UTACC system.
- Each component of the UTACC system will be networked to facilitate data sharing.
- Insider threats are already prevalent in every information and unmanned systems in the DOD and this threat has been mitigated to an acceptable level of risk through our current policies, education and training.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
  - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
  - Continue development of the UTACC concept of operations.
  - Conduct extensive testing and evaluation with operational units.
  - Assess and mitigate Insider Threats through training requirements prescribed by the DOD and the USMC.
  - Research approaches used by other weapons and information systems.
- Technical Controls
  - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
  - Implement cryptographic solutions:
    - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
    - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
  - Implement access controls through authentication (Login Information, Passwords, and Biometrics).
  - Implement access control through privileges (System administrators, users, etc).
  - Implement a "two person rule" for system administrators to reduce errors and

tampering.
- Research and employ tamper resistant technology.
- Implement a remote zeroing capability of software, data, and cryptographic material.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PHISHING

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
People and Operations	Phishing

THREAT SUMMARY

Phishing is an attempt to gain sensitive information such as usernames and passwords from an individual by impersonating a legitimate entity. In many cases this takes place in an email that is impersonating a legitimate entity, asking the target individual to verify information (banking numbers, SSN, etc) [37]. In the case of UTACC the attack would specifically target personnel that maintain, operate or have direct contact with the UTACC system in order to expose vital access data for the system. This data could include administrative user names, passwords, and personal identification numbers (PIN).

The most dangerous threat permutation would be an attacker gaining access to information enabling them to control the UTACC system, destroy it, and / or steal sensitive information. An example of this would an email that appears to be from a system manufacturer (General Dynamics or Lockheed Martin) stating that there is a problem with the UTACC system that can be fixed remotely as long as the usernames and passwords are included in a reply email. If a reply email is sent the unauthorized user acquires access to the entire UTACC system.

The most likely threat impact would be an attacker gaining access information, using the same method stated above, enabling temporary access to change settings or parameters that in turn would reduce the UTACC's mission capability and effectiveness.

IMPACTS TO THE CIA TRIAD

- Phishing is a direct threat to confidentiality, but could also impact integrity and availability [32].

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The UTACC system will require some form of physical security to protect cryptographic material and keys.
- Network access is a requirement for the UTACC system.

- Each component of the UTACC system will be networked to facilitate data sharing.
- Phishing threats are already prevalent in every information and unmanned systems in the DOD and this threat has been mitigated to an acceptable level of risk through current policies, best common practices, education and training.

SECURITY CONTROLS

- Non-technical Controls
    - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
    - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
    - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
    - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
    - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
    - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
    - Continue development of the UTACC concept of operations.
    - Conduct extensive testing and evaluation with operational units.
    - Assess and mitigate Phishing threats through training requirements prescribed by the DOD and the USMC.
- Technical Controls
    - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
    - Implement cryptographic solutions:
        - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
        - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
    - Implement access controls through authentication (Login Information, Passwords, and Biometrics).
    - Implement access control through privileges (System administrators, users, etc).
    - Implement a "two person rule" for system administrators to reduce errors and tampering.
    - Employ and research tamper resistant technology.
    - Implement a remote zeroing capability of software, data, and cryptographic

material.

- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. MAINTENANCE OF THE UTACC SYSTEM

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
People / Operations	Maintenance of the UTACC System

THREAT SUMMARY

This threat stands against the ability of a unit to own and maintain the UTACC system. Without proper maintenance and accountability the UTACC system will rarely, if ever, be 100% mission ready. The maintenance process needs to be extensively researched before acquiring and distributing the UTACC system to the Fleet Marine Force (FMF). This system is extremely unique because it is composed of parts and components that traditionally are owned by multiple agencies within the Marine Air Ground Task Force (MAGTF). This could result in multiple supply chains, which confuse and slow maintenance processes. A look at current maintenance procedures of current Unmanned Aerial Systems (UAS) employed by the Marine Corps will offer maintenance options for the UTACC system.

The examples provided offer two distinct methods of maintaining an unmanned system, like UTACC. An example of split maintenance /and supply chains is seen currently in the USMC with the Shadow UAS. The Air Combat Element (ACE) provides aviation supply support to Marine Unmanned Aerial Vehicle Squadron (VMU) aviation assets, such as the Unmanned Aerial Vehicles (UAV) and the Ground Control Stations (GCS) [38]. The VMU squadron's non-aviation assets (radios, vehicles, generators) are provided through the existing Marine Corps system for provisioning and supplies [38]. This is a cause for consternation and confusion in current VMUs. In contrast, the Raven UAS is owned, operated, and maintained by Marine infantry battalions [38]. The responsibility of one entity for this technology streamlines the maintenance process to a single system. This streamlined maintenance process would be the simplest way to integrate the UTACC system into MAGTF operations from a maintenance standpoint.

An infantry or reconnaissance battalion possesses enough organic support to maintain a system, like UTACC. These units have the following organic assets available (Intelligence, Communications (EKMS), Ground / Air Operation planners, Logistics (Maintenance), and Supply) to assist in planning, operations, and maintenance of the system. Operationally the UTACC system is being designed to support small teams or squads who will employ and operate the system, which will be supported through infantry or reconnaissance battalions.

The most dangerous threat impact to the UTACC's maintenace readiness is the potential for the system to be fieided without a plan to train Marines on the UTACC system maintenance procedures. In this example the UTACC system is delivered to an operational unit and none of the Marines have completed the required maintenance training. The UTACC system in inoperable and must be inducted into the maintenance cycle, but the unit does not possess qualified maintainers to repair the system.

The most likely threat possibility is that replacement parts and components are not readily available in the supply system when UTACC is delivered for operational employment. An example would be that a UTACC system component fails during operations and the Marines must wait an extended period to receive a replacement component. The result is a non-mission capable system until the part is received, installed, and tested.

IMPACTS TO THE CIA TRIAD

- Improper maintenance could lead to a system crash, which is a threat to data availability [32].

IMPACTS TO UTACC
VULNERABILITY ANALYSIS • When the UTACC system is fielded to operational units.
ASSUMPTIONS • Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member. • The UTACC system will be supported through a Marine Corps or Navy supply system.
SECURITY CONTROLS • Non-technical Controls o Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system. o Establish a training pipeline for maintenance that will support the UTACC system employment by a USMC unit. o Continue development of the UTACC concept of operations. o Conduct extensive testing and evaluation with operational units. o Develop a detailed maintenance plan that is vetted by an operational FMF unit owns the UTACC system. o Conduct a detailed review of the RQ-7B Shadow, RQ-11 STUAS, and RQ-11 Raven UASs programs and their approach to maintenance and ownership of the systems. o Research the utilization of three-dimensional printing solutions to provide replacement parts for UTACC. o Research and implement simple user maintenance techniques. • Technical Controls o Research and implement remote monitoring techniques for diagnostics and system usage.

APPENDIX D. ATTITUDE TOWARDS EMERGING TECHNOLOGIES

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
People	Attitude Towards Emerging Technologies

THREAT SUMMARY

The Marine Corps does not readily accept anything new unless it is a proven asset and provides an exceptional capability. The USMC has always made do, and accomplished their mission, with less equipment, technology, money, and people. The Marine Corps does not normally lead in developing advanced technology for combat operations. Technological advancements take time to mature to a level of reliability for utilization in combat. An example of a technological advancement reaching maturity would be the Advanced Research Project Agency Network (ARPANET). The ARPANET was the first computer network and was developed in the 1960s [39]. The ARPANET took roughly forty years to mature into the networks that are currently employed in support of combat operations in Afghanistan and Iraq. Marines are now comfortable with utilizing computer networks in combat operations and the UTACC system must reach the same level of reliability to be relevant to the Marine Corps.

The authors have observed that when new technologies are fielded to the USMC, the initial perception of Marines receiving the technology is that it will be an additional burden to the unit especially with regards to maintenance, accountability, and operational capability. If fielded improperly without proven operational capabilities, extensive training packages, and a solid maintenance plan the UTACC system will be quickly discarded to sit on a shelf. When lives hang in the balance Marines will trust technology they understand and can physically see as a combat multiplier. An autonomous robot on the battlefield will initially be seen as a threat to mission success and the lives of Marines. Another issue affecting the credibility of UTACC is the unproven autonomous and user interface technology required by the system.

The user interface technology, which is entirely new and requires the development of a new concept of operations to integrate this technology into a Marine Corps unit. This newly developed Human Marine Interaction (HMI) software must earn the trust of Marines before it will ever be employed. The final configuration of UTACC is intended to be a decision-centric, semi-autonomous, distributive, multi-agent, and multi-domain robotic system [28]. UTACC will require HMI between Marines and all system components. The interaction required for UTACC to provide capabilities would be the same interaction required between team members. Robots have not been able to demonstrate the abilities of a teammate and therefore would not be employed by a small unit in combat because it is not a proven technology [40]. UTACC technology must be heavily researched, developed, and tested to meet the unique and rigorous demands of a reconnaissance team.

The most dangerous impact of this threat to the UTACC system would be the procurement and failure to utilize the system, due to the lack of confidence in new equipment and technologies. The Marine Corps will not procure or utilize the UTACC system if the system does not produce a consistent and reliable set of capabilities.

The most likely variation of this threat is that the system will be underutilized. An example of this would be the UTACC never being fully integrated into the commander's Command and Control (C2) process as a result of increased equipment maintanance due to training shortfalls.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the Marine Corps culture toward emerging technology is not swayed the system will not be procured by the USMC.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- During demonstrations of UTACC that showcase capabilities for potential units.
- Integration of the UTACC system during training exercises.
- Insufficient training pipelines for the UTACC system.

ASSUMPTIONS

- If this plan is not vetted by an operational unit with a vested interest, this concept will not be fully researched or developed.

SECURITY CONTROLS

- Non-technical Controls
    - Analyze current and future DOD and USMC policies, procedures and publications must to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system
    - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
    - Educate leaders and key decision makers on the UTACC system technology and capabilities.
    - Demonstrate the capabilities of the UTACC to Fleet Marine Force personnel and commands.
        - The UTACC system must validate reliability while highlighting capabilities during demonstrations. Results and conclusions of these demonstrations, plus theses, point papers and briefs should be published by the Marine Corps Warfighting Lab to operational units.
    - Research the ability to incorporate current operational or program of record unmanned systems into the UTACC system. Marines have familiarity with these systems.
    - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
    - Continue development of the UTACC concept of operations.
    - Conduct extensive testing and evaluation with operational units.
    - Develop the UTACC system ensuring ease of use for Marines.
- Technical Controls
    - Employ mandatory semi-autonomous modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.

APPENDIX E. AUTONOMY AS AN ETHICAL CONCERN

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
People	Autonomy as an Ethical Concern

THREAT SUMMARY

Autonomy is a capability or a set of capabilities that allows certain actions of a system to be automatic while remaining inside the boundaries of a program. At the most basic level, autonomy requires trust. We trust autonomous systems to route emails and assign Internet Protocol (IP) addresses. Autonomy is even trusted in the Shadow UAS tactical automated landing system (TALS), which automatically lands the UAV without human interaction [38]. The level of autonomy illustrated in these examples are minor compared to the level of autonomy planned for the UTACC system. The amount of trust the UTACC requires to operate effectively is equal to the trust between Marines. The trust amongst Marines is developed over time due to training and familiarity with one another. Extensive training packages would be the format for introducing UTACC and over time the Marines would gain trust in the system.

Semi-autonomous operations have a human in the loop, while full autonomy is the completion of a task or mission without human involvement other than mission assignment [41]. The threat of ethical considerations arises when we take a human out of the loop and allow technology to make its own decisions in a combat environment. This environment includes friendly forces, enemy forces, and civilian non-combatants. The technology by itself must be programmed to deal with different groups of people and could include interaction, avoidance, confrontation, etc. Programming cannot anticipate every situation the UTACC system will encounter. Accidents are expected to occur given the technical limitations of programming a robot with the ability to effectively distinguish valid and invalid targets, which raises the question of legal responsibility [42]. If a weapons system is added to the UTACC system, then an additional layer of ethical concern is added to the equation.

The most dangerous variation of this threat would be the UTACC system being employed and becomming a physical threat to personnel (friendly/non-combatant). An example of this would be the UTACC Unmanned Ground Vehicle (UGV) being surrounded by a group of civilians and the UGV being unable to move away from the crowd. The UGV might choose to move away from the crowd using the least blocked path which includes running over a small child as the child is caluclated to be the smallest obstacle.

The most likely threat possibility is that the system will be underutilized for fear of a physical threat to personnel. An example of this would be never using the UTACC system in an urban environment where it will encouner civilian popluations, due to fear of the system harming innocent civilians.

IMPACTS TO THE CIA TRIAD

- If ethical concerns arise concerning the employment of the UTACC system it will be impact the availability of the system.
-

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- When the UTACC system is employed in any environment.

ASSUMPTIONS

- If this plan is not vetted by an operational unit with a vested interest, this concept will not be fully researched or developed.
- The USMC will accept responsibility for the actions or inactions of the UTACC system.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications must to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
  - Continue development of the UTACC concept of operations.
  - Conduct extensive testing and evaluation with operational units.
  - Conduct a detailed review of the RQ-7B Shadow, RQ-11 STUAS, and RQ-11 Raven UASs programs and their approach to fully autonomous modes of operation.
  - Enlist NPS and Federally Funded Research Development Centers (FFRDC) to conduct research on the ethics of autonomous unmanned operations.
- Technical Controls
  - Employ mandatory semi-autonomous modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
  - Implement independent UGV and UAV operations.

APPENDIX F. SPYWARE

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Spyware

THREAT SUMMARY

Spyware is software that monitors and gathers data about an organization, individual, or entity without their knowledge and enables a third party to access the data [43]. The UTACC system will be vulnerable to spyware and if infected, the system will release sensitive data (telemetry data, map data, metadata) to our enemies without our knowledge. Spyware is a very serious problem and has caused more than 50 percent of the failures of the Microsoft Windows operating system [43]. The UTACC system will require some form of an operating system to enable Marine interaction. Application-based spyware can open a channel to install upgrades and additional applications without user permission or knowledge [43]. All new mobile devices are application based and UTACC will have applications for end users, making it susceptible to this type of spyware.

Spyware has adapted to the mobile world and will eventually target vehicles once they are integrated into the Internet [44]. Vehicles connected through networking are the basis for the UTACC system operation and collaboration. Vehicle Area Networks (VANET) require constant interaction with onboard sensors and spyware might track vehicles by conducting passive sensor-based attacks [44].

The most dangerous threat impact of spyware to UTACC would be an enemy gaining the ability locate our friendly forces due to infiltration into the UTACC system. For instance the enemy could develop spyware to acquire telemetry data from the UTACC. This data might help the enemy to locate the UTACC system and the Marines employing the system.

The most likely possible threat of spyware would be application-based spyware installing updates and modifications to the UTACC system without the knowledge of the Marines. The system would eventually experience a failure with the operating system, making the system non-mission capable.

IMPACTS TO THE CIA TRIAD

- This threat if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The UTACC system will require some form of physical security to protect cryptographic material and keys.
- Network access is a requirement for the UTACC system.
- Each component of the UTACC system will be networked to facilitate data sharing.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
  - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
  - Continue development of the UTACC concept of operations.
  - Conduct extensive testing and evaluation with operational units.
  - Research approaches used by other weapons and information systems.
- Technical Controls
  - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
  - Implement cryptographic solutions:
    - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].

        - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
    - Implement access controls through authentication (Login Information, Passwords, and Biometrics).
    - Implement access control through privileges (System administrators, users, etc).
    - Implement a "two person rule" for system administrators to reduce errors and tampering.
    - Research and employ tamper resistant technology.
    - Implement a remote zeroing capability of software, data, and cryptographic material.
    - Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G. JAMMING OF COMMAND AND CONTROL AND DATA LINKS

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Jamming of Command and Control and Data Links

THREAT SUMMARY

Electronic attack is the division of electronic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack equipment (UTACC) [45]. The UTACC system must be functional in an environment where our enemy can jam our command and control and information communication links. A near peer enemy will have jammers that can affect the entire frequency spectrum.

A focus of UTACC system developers and designers should be electronic protection that focuses on passive and active means to protect equipment from friendly or enemy employment of electronic warfare that degrades, neutralizes, or destroys friendly combat capability [45]. The UTACC will be exposed to electronic attack and the common threat of jamming communication links must be addressed and mitigated. When a transmitter-receiver pair communicates, a jammer can corrupt the data and make it unreadable at the receiver side [46].

The most dangerous threat possibility during an electronic attack would be the UTACC system being targeted by enough directed energy to cause electronic component failure while in operation. The Unmanned Ground Vehicle (UGV) is discovered by enemy ground forces and a directed energy device is directed at the UGV and all the onboard electronic systems are damaged. If the UGV is required for Unmanned Aerial Vehicle (UAV) operations and information exchange, the UAV will be rendered ineffective.

The most likely threat impact would be the enemy electronically jamming a certain band of the frequency spectrum, rendering it unusable for a certain amount of time. For example, the enemy could jam a portion of the C-Band frequency spectrum, rendering the video feeds in that portion of the spectrum useless.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- The UTACC system is required to utilize portions of the frequency spectrum to conduct operations.

SECURITY CONTROLS

- Non-technical Controls
    - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
    - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
    - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
    - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
    - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
    - Continue development of the UTACC concept of operations.
    - Conduct extensive testing and evaluation with operational units.
    - Research approaches used by other weapons and information systems.
    - Conduct extensive research of the electromagnetic (EM) spectrum; identify frequency bandwidth requirements of the system, identify portions of the EM spectrum available for use, identify enough EM spectrum to facilitate frequency hopping to mitigate jamming.
    - Coordinate with USMC and DOD frequency management officials to ensure frequency availability.
    - Research the utilization of cognitive radios that seek open spectrum and ensure they are in compliance with USMC COMSEC procedures and the USMC and DOD frequency management policies.
- Technical Controls
    - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.

- Employ a fully autonomous get home control mode of operation (Shadow UAS).
- Implement redundant and encrypted C2 and data links spread across the EM spectrum.
- Implement independent UGV and UAV operations to mitigate the effects if one portion of the UTACC system is jammed.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H. DENIAL OF SERVICE ATTACK

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Denial of Service Attack

THREAT SUMMARY

A denial of service attack incapacitates networks through saturation and bandwidth consumption (i.e sendmail buffer overflow, pipe attacks, MIMEbo, Syn flood) [32]. This attack can be used against a system like UTACC to render the system inoperable. The denial of service threat against the UTACC system could utilize an internal routing protocol between the Unmanned Aerial Vehicle (UAV)/Unmanned Ground Vehicle (UGV) or any router or routing protocol between any components of the UTACC system. The denial of service attack would render the internal routers of the system useless, therefore causing the system not to process or route data to key components of the UTACC system and to decision makers.

The most dangerous threat permutation would be the enemy discovering a vulnerability in the routing protocols within the UTACC system. The unauthorized user then could develop a denial of service attack to specifically target the UTACC system routing protocols, rendering the system fully inoperable. This attack vector, once discovered could be employed against every UTACC system until a security patch is installed. For example if the UTACC system is on an operational network and the systems' routing protocols are specifically targeted by hackers this could cause the systems to become inoperable.

The most likely threat impact would be periods of non-operability while patches are installed for denial of service attacks on popular routing protocols used by many systems, including UTACC. A security patch for the denial of service attack would likely be developed prior to the UTACC systems being affected. An example would be that an attacker would attack a certain vulnerability in a popular wireless routing protocol utilized by many systems. While the security patch is being develped, distributed, and installed the UTACC system would be non-operational.

IMPACTS TO THE CIA TRIAD

- This attack can impact availability and integrity of resources and data [32].

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The UTACC system will require some form of physical security to protect cryptographic material and keys.
- Network access is a requirement for the UTACC system.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- Each component of the UTACC system will be networked to facilitate data sharing.

SECURITY CONTROLS

- Non-technical Controls
    - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
    - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
    - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
    - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
    - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
    - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
    - Continue development of the UTACC concept of operations.
    - Conduct extensive testing and evaluation with operational units.
- Technical Controls
    - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
    - Implement cryptographic solutions:
        - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires

significant infrastructure [36].
        - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
    - Implement access controls through authentication (Login Information, Passwords, and Biometrics).
    - Implement access control through privileges (System administrators, users, etc).
    - Implement a "two person rule" for system administrators to reduce errors and tampering.
    - Research and employ tamper resistant technology.
    - Implement a remote zeroing capability of software, data, and cryptographic material.
    - Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I. EAVESDROPPING

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Eavesdropping

THREAT SUMMARY

Eavesdropping occurs when a transmitter sends data to a receiver and the data is received by anyone other than the intended recipient; eavesdropping is almost impossible to detect [46]. Eavesdropping can occur on wired and wireless communications links. The UTACC system will employ wireless Command and Control (C2) and data links, enabling the eavesdropping threat. Eavesdropping is conducted in myriad ways including electronic bugs, applications such as Trojan horses, packet sniffers, and amplifiers on unprotected cables [32]. In the case of UTACC, eavesdropping could take place when the data is being passed from the UTACC system to the Marines or between the UTACC system components. Current Marine Corps Unmanned Aerial Systems (UAS) do not properly mitigate this threat because their C2 and data links are not currently encrypted [38]. The UTACC system must mitigate this threat to an acceptable level because eavesdropping can lead to more serious threats. An example of more serious attacks include viruses or malicious code that may compromise a wireless device and subsequently impact a wired network [47].

The most dangerous situation would be an attacker eavesdropping on the UTACC system and being able to discern critical information about the system, like Internet Protocol (IP) addresses. The attacker then could masquerade the Internet Protocol (IP) address and gain access to the Secret Internet Protocol Router Network (SIPRNET). The attacker could then employ a virus to attack the SIPRNET by gaining access through the UTACC system.

The most likely threat impact would be an attacker eavesdropping on a certain frequency and being able to hear or see noise, but is unable to distinguish the data or information on the frequency.

IMPACTS TO THE CIA TRIAD

- Eavesdropping impacts data confidentiality; but when combined with other threats could impact data integrity and availability [32].

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The UTACC system will require some form of physical security to protect cryptographic material and keys.
- Network access is a requirement for the UTACC system.
- Each component of the UTACC system will be networked to facilitate data sharing.
- Eavesdropping will happen regardless and this threat must be mitigated.

SECURITY CONTROLS

- Non-technical Controls
    - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
    - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
    - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
    - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
    - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
    - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
    - Continue development of the UTACC concept of operations.
    - Conduct extensive testing and evaluation with operational units.
- Technical Controls
    - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
    - Implement cryptographic solutions:
        - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].

        - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
    - Implement access controls through authentication (Login Information, Passwords, and Biometrics).
    - Implement access control through privileges (System administrators, users, etc).
    - Implement a "two person rule" for system administrators to reduce errors and tampering.
    - Research and employ tamper resistant technology.
    - Implement a remote zeroing capability of software, data, and cryptographic material.
    - Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).
    - Research the utilization of sensors that detect eavesdropping.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX J. AN ATTACK ON MOBILE DEVICES ON A WIRELESS NETWORK

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	An Attack on Mobile Devices on a Wireless Network

THREAT SUMMARY

This threat is aimed at the mobile devices a UTACC system will use to store, transmit, and receive sensitive data to allow for UTACC operations. To analyze this threat, this template will compare these components of the UTACC system to common mobile devices (smart phones, tablets, laptop computers), since significant research has been conducted on these devices. Mobile devices offer a significant area of vulnerability to UTACC. Mobile devices are small and portable which make them easily obtainable through theft or misplacement by the owner, enabling the discovery of sensitive data stored on the device [47].

The data that will be stored on the UTACC system mobile components will require sophisticated protection schemas to ensure the data is not compromised. If a mobile device is stolen or lost and still has network connectivity the entire network is now exponentially more vulnerable to exploitation. Viruses or malicious code may compromise a wireless device and successively impact the wired network [47]. Once the enemy or attacker has possession and access to mobile device, they are able to access the network and affect more than the data on the device.

The most dangerous threat scenario would be the enemy gaining access to the Secret Internet Protocol Router Network (SIPRNET) through a lost or stolen mobile device associated with the UTACC system which has retained network connectivity. An example would be a Marine losing a UTACC mobile device. The enemy is able to acquire and gain access to the lost mobile device and the network and upload a virus causing a network outage.

The most likely threat impact would be that a lost mobile device is obtained by our enemy who is able to gain access to the classified information stored on the mobile device. The enemy or attacker is able to crack the encryption schema device, unlocking all the information on the device. The device no longer has network connectivity because it was reported lost and blacklisted from the network. The enemy now has potentially valuable information that was stored on the mobile device.

IMPACTS TO THE CIA TRIAD

- This threat if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC
VULNERABILITY ANALYSIS • UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.
ASSUMPTIONS • Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member. • The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented. • The UTACC system will require some form of physical security to protect cryptographic material and keys. • Network access is a requirement for the UTACC system. • The system has to be able to be left behind in the event of an emergency or loss of life. • Each component of the UTACC system will be networked to facilitate data sharing. • Marines will utilize mobile devices to employ the UTACC system.
SECURITY CONTROLS • Non-technical Controls o Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system. o Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies. o Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA. o Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security. o Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security o Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit. o Continue development of the UTACC concept of operations. o Conduct extensive testing and evaluation with operational units. • Technical Controls

- Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
- Implement cryptographic solutions:
  - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
  - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
- Implement access controls through authentication (Login Information, Passwords, and Biometrics).
- Implement access control through privileges (System administrators, users, etc).
- Implement a "two person rule" for system administrators to reduce errors and tampering.
- Research and employ tamper resistant technology.
- Implement a remote zeroing capability of software, data, and cryptographic material.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).
- Implement separate boot files for specific missions to decrease data stored on the UTACC system.
- Research and consider organic local data processing and deletion techniques to minimize data storage onboard UTACC.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX K. A COMPUTER VIRUS ATTACK ON THE UTACC SYSTEM

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Computer Virus Attack on the UTACC System

THREAT SUMMARY

Computer viruses have developed over time from programs such as Trojan horses and logic bombs [48]. A computer virus infects software programs in order to alter, erase, destroy, or reveal critical information to benefit the attacker [48]. Computer viruses can be developed to target a wide range of software programs or can be specifically developed to exploit a specific software. The Stuxnet virus was designed to specifically target Siemens industrial control systems, which were employed by Iranian nuclear reactors [49].

Our enemies have multiple methods to employ viruses against UTACC. The first method is enabled through geographical co-location between the enemy and Unmanned Ground Vehicle (UGV). The enemy is able to upload the virus through a physical connection to the UGV. Viruses or malicious code may compromise a wireless device and subsequently impact a wired network [47]. The second method would be accessing the UTACC system virtually through wired and wireless networks.

The most dangerous threat permutation would be the enemy constructing a computer virus specifically designed to attack the UTACC system. An example would be that the UGV is located by the enemy and a computer virus is uploaded into the UGV. The virus replicates to other UTACC systems being employed through network connectivity and all become infected with the virus. The virus, once spread, can enable the enemy to conduct attacks on personnel, equipment, and data.

The most likely threat situation would be that the UTACC system is subjected to a computer virus not specifically designed to attack UTACC. An example would be the UGV is discovered and a virus is uploaded onto the UGV which attempts to send information to attackers. The virus is discovered by network administrators at the firewall, because the data traffic is suspicious. Once discovered the UTACC system in question is isolated and the virus is removed.

IMPACTS TO THE CIA TRIAD

- This threat if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC
VULNERABILITY ANALYSIS • UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.
ASSUMPTIONS • Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member. • The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented. • The UTACC system will require some form of physical security to protect cryptographic material and keys. • Network access is a requirement for the UTACC system. • The system has to be able to be left behind in the event of an emergency or loss of life. • Each component of the UTACC system will be networked to facilitate data sharing.
SECURITY CONTROLS • Non-technical Controls o Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system. o Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies. o Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA. o Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security. o Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security o Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit. o Continue development of the UTACC concept of operations. o Conduct extensive testing and evaluation with operational units. • Technical Controls o Employ mandatory semi-autonomous (man-in-the-loop) modes of

operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.

- Implement cryptographic solutions:
  - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
  - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
- Implement access controls through authentication (Login Information, Passwords, and Biometrics).
- Implement access control through privileges (System administrators, users, etc).
- Implement a "two person rule" for system administrators to reduce errors and tampering.
- Research and employ tamper resistant technology.
- Implement port security for all external hardware connections (RG-45 ethernet) to prevent unauthorized hardwire access to system components and information.
- Implement a remote zeroing capability of software, data, and cryptographic material.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX L. IMPERSONATION OR SPOOFING AN UNMANNED GROUND VEHICLE (UGV) OR UNMANNED AERIAL VEHICLE (UAV)

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Impersonation or Spoofing an Unmanned Ground Vehicle (UGV) or Unmanned Aerial Vehicle (UAV)

THREAT SUMMARY

Impersonation or "spoofing" occurs when an illegitimate transmitter sends both correct and incorrect information, fooling the receiver into processing the illegitimate data [46]. A near-peer enemy has the technology available to spoof or impersonate a component of the UTACC system due to the system requirements for wireless communication links. The absence of a certification authority in ad hoc wireless networks allows a malicious node to spoof the identity of any node [47]. If the UGV is discovered or the enemy conducts a Radio Frequency (RF) spectrum analysis to determine the frequencies utilized by the UTACC system, then a receiver-transmitter can be constructed to impersonate the UGV and send false or incorrect information to the UTACC system and components.

The most dangerous threat scenario would be the enemy gaining access to the specifications of the UTACC system and developing a receiver-transmitter to spoof the UGV. The enemy could locate and turn the UTACC UGV off while simultaneously turning on their illegitimate receiver-transmitter. The enemy could now receive UTACC system information or insert false information into the UTACC system, affecting decision making by the system or Marines.

The most likely threat possibility would be the enemy constructing a receiver-transmitter which would jam the UTACC system, without actually receiving information from or injecting false information into the system. The system would automatically switch to the secondary command and contol link or enter a fully autonomous "get home control mode" enabling UTACC to return to a predetermined location without human interaction.

IMPACTS TO THE CIA TRIAD

- This threat if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- Wireless communication links will be utilized by the UTACC system.
- The UTACC system will require some form of physical security to protect cryptographic material and keys.
- Network access is a requirement for the UTACC system.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- Each component of the UTACC system will be networked to facilitate data sharing.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
  - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
  - Continue development of the UTACC concept of operations.
  - Conduct extensive testing and evaluation with operational units.
- Technical Controls
  - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
  - Implement cryptographic solutions:
    - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept

secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
        - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
- Implement access controls through authentication (Login Information, Passwords, and Biometrics).
- Implement access control through privileges (System administrators, users, etc).
- Implement a "two person rule" for system administrators to reduce errors and tampering.
- Research and employ tamper resistant technology.
- Implement a remote zeroing capability of software, data, and cryptographic material.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).
- Implement redundant and encrypted C2 and data links spread across the EM spectrum.
- Implement a fully autonomous get home control mode of operation (Shadow UAS).
- Research alternative mobile ad-hoc networking protocols and strategies.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX M. SPOOFING AN INTERNET PROTOCOL (IP) OR MEDIA ACCESS CONTROL (MAC) ADDRESS OF A UTACC SYSTEM COMPONENT

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Spoofing an Internet Protocol (IP) or Media Access Control (MAC) Address of a UTACC System Component.

THREAT SUMMARY

The UTACC system will employ IP/MAC addresses to route data between different components of the UTACC system. Spoofing an IP or MAC address is a common occurrence on computer networks. This type of attack is a viable option for attacking the UTACC system. MAC spoofing is the process of observing network traffic to obtain a legitimate MAC address and then impersonating that legitimate address [50]. MAC addresses can provide attackers with IP addresses of the spoofed computer through Address Resolution Protocol (ARP) [50]. IP spoofing is a process used by attackers to gain network layer access to computers, by sending packets to a computer with a spoofed IP address of a trusted and legitimate host [50]. An attacker can capture packets to determine IP / MAC addresses and then modify the header information to show the packets are coming from a trusted IP /MAC address. The attacker could use their obtained access to insert viruses, employ a denial of service attack, or conduct a man-in-the-middle attack.

The most dangerous threat possibility would be an attacker spoofing an IP or MAC address of a UTACC system component and being able to conduct an attack on the entire network. An example would be that the attacker is eavesdropping on the wireless communication between UTACC system components and is able to obtain the IP address of the Unmanned Ground Vehicle (UGV). This UTACC is wirelessly connected to the network. The attacker spoofs the IP address of the UGV and is able to connect to the network and gains access to launch more significant attacks.

The most likely threat impact would be an attacker spoofing a IP or MAC address of the UTACC system and being able to observe data transmitted and received by other components of the UTACC system without impacting the entire network. An example would be an attacker spoofing the IP address of the Unmanned Aerial Vehicle (UAV) and gaining the ability to receive information from the UGV.

IMPACTS TO THE CIA TRIAD

- This threat if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC
VULNERABILITY ANALYSIS • UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.
ASSUMPTIONS • Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member. • The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented. • The UTACC system will require some form of physical security to protect cryptographic material and keys. • Network access is a requirement for the UTACC system. • The system has to be able to be left behind in the event of an emergency or loss of life. • Each component of the UTACC system will be networked to facilitate data sharing.
SECURITY CONTROLS • Non-technical Controls o Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system. o Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies. o Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA. o Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security. o Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security o Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit. o Continue development of the UTACC concept of operations. o Conduct extensive testing and evaluation with operational units. • Technical Controls o Employ mandatory semi-autonomous (man-in-the-loop) modes of

operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.

- Implement cryptographic solutions:
  - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
  - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
- Implement access controls through authentication (Login Information, Passwords, and Biometrics).
- Implement access control through privileges (System administrators, users, etc).
- Implement a "two person rule" for system administrators to reduce errors and tampering.
- Research and employ tamper resistant technology.
- Implement a remote zeroing capability of software, data, and cryptographic material.
- Research alternative mobile ad-hoc networking protocols and strategies.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX N. UNPROTECTED INFORMATION STORED ON THE UTACC SYSTEM

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Unprotected Information Stored on the UTACC System

THREAT SUMMARY

The UTACC system will store data and information processed by onboard sensors. The information will be utilized by Marines to make decisions. If the information is not protected, then it is vulnerable to manipulation. The UTACC concept of operations places the system in the same place as the enemy, which enables access to system data and information. The UTACC will be the first system where unmanned air and ground vehicles collaborate to complete a task. The UGV portion of the UTACC system will be geographically co-located with enemy forces. The most commonly employed autonomous vehicles are Unmanned Aerial Vehicles (UAV) and they are not easily accessible by enemy forces. When the UTACC system is employed, the enemy may be able to obtain data and information stored onboard the UTACC system which could impact operations and security. Information security is the protection of information and information systems against unauthorized access or modification of information and must be achieved to enable employment of the UTACC system [29].

The most dangerous threat possibility would be the UTACC system not employing an encryption solution and system information being accessed by the enemy. The enemy could utilize the information to locate and attack Marines. Most unmanned systems are not required to complete the DIACAP to be employed, which increases vulnerabilities and limits capabilities of the systems.

The most likely threat possibility is the UTACC system is developed and because the system cannot attain a DIACAP certification an encryption solution is added as an afterthought instead of as a guiding principle. The system will experience an increase in cost and longer acquisition timelines.

IMPACTS TO THE CIA TRIAD

- These threats if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of

an operational team member.

- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The system will require some form of physical security to protect cryptographic material and keys.
- Network access is requirement for the UTACC system.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- Each component of the UTACC system will be networked to facilitate data sharing.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
  - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
  - Conduct extensive testing and evaluation with operational units.
- Technical Controls
  - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
  - Implement cryptographic solutions:
    - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
    - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
  - Implement access controls through authentication (Login Information, Passwords, and Biometrics).
  - Implement access control through privileges (System administrators, users, etc).
  - Implement a "two person rule" for system administrators.
  - Research and employ tamper resistant technology.
  - Implement port security for all external hardware connections (RG-45 ethernet) to

prevent unauthorized hardwire access to system components and information.

- Implement a remote zeroing capability of software, data, and cryptographic material.
- Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).
- Research and consider organic local data processing and deletion techniques to minimize data storage onboard UTACC.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX O. FREQUENCY MANAGEMENT AND DE-CONFLICTION

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Frequency Management and De-confliction

THREAT SUMMARY

Electromagnetic (EM) operations involve operational planning and frequency management [29]. Operational planning is the ability to integrate EM spectrum-dependent systems in support of missions, and mitigate friendly or harmful interference [29]. UTACC must be integrated into the EM operational plan to mitigate interference. Frequency management is the process of requesting, recording, de-conflicting, and authorizing the frequencies for use [29]. The UTACC system must be allocated enough of the EM spectrum to operate effectively. The allocation of the EM spectrum must be sufficient to support frequency hopping to combat jamming, and to support redundant command and control (C2) and data links to each of the operational UTACC systems. Open frequencies are becoming less available, due to the amount of systems requiring the EM spectrum to perform critical tasks.

The UTACC system engineers and designers must research and identify open blocks of frequencies that meet the requirements of the UTACC system bandwidth to effectively mitigate frequency management issues. Frequency management issues will only worsen over time due to the constant process of acquiring new systems and equipment utilizing the EM spectrum.

The most dangerous threat impact would be failing to properly identify UTACC frequency requirements before conducting the appropriate research of the EM spectrum. In this scenario, UTACC is funded and fielded but the Marines would be unable to obtain enough frequencies to operate the system in certain situations or environments. An example would be an insufficient frequency allocation to employ a frequency hopping technique to mitigate enemy jamming. The system is jammed and rendered combat ineffective.

The most likely threat possibility would be that the development process is disrupted because research reveals the UTACC system specifications must change to ensure EM spectrum integration. For instance, the engineers and designers might determine that the UTACC system will utilize the L-band portion to meet system requirements, but find that this portion is extremely congested and the required spectrum cannot support the UTACC system. The engineers and designers are forced to use the C-band portion of the EM spectrum which requires different antennas and receiver-transmitters.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- When the UTACC system is designed, developed, and employed.

ASSUMPTIONS

- The UTACC system will require frequencies to properly operate.
- The system will employ frequency hopping schemes to defeat jamming.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
  - Continue development of the UTACC concept of operations.
  - Conduct extensive testing and evaluation with operational units.
  - Research approaches used by other weapons and information systems.
  - Conduct extensive research of the electromagnetic (EM) spectrum; identify frequency bandwidth requirements of the system, identify portions of the EM spectrum available for use, identify enough EM spectrum to facilitate frequency hopping to mitigate jamming.
  - Coordinate with USMC and DOD frequency management officials to ensure frequency availability.
  - Research the utilization of cognitive radios that seek open spectrum and ensure they are in compliance with USMC COMSEC procedures and the USMC and DOD frequency management policies.
- Technical Controls
  - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.
  - Employ a fully autonomous get home control mode of operation (Shadow UAS).
  - Employ redundant and encrypted C2 and data links spread across the EM spectrum.
  - Implement independent UGV and UAV operations to mitigate the effects if one portion of the UTACC system is jammed.

APPENDIX P. UTACC SYSTEM INTEGRATION WITH LEGACY AND NEWLY PROCURED SYSTEMS

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	UTACC System Integration with Legacy and Newly Procured Systems

THREAT SUMMARY

The UTACC system must be interoperable and communicate with legacy and newly fielded systems to enable collaboration and information sharing across the battlespace. The integration of systems is a difficult goal to accomplish in any enterprise, but more so in a large organization like the Marine Corps. Integration of software systems has become one of the most important and resource-consuming measures in software management [51]. The equipment procured in the next ten to fifteen years is still in the developmental stages, much like UTACC. An example of failed integration was the incompatibility of KC-130J Harvest Hawk weapons systems with the Remote Optical Video Enhanced Receiver (ROVER) III due to the downlink frequency on the KC-130J [52]. This was corrected when a new version of the ROVER was fielded, but possibly could have been avoided had the system been properly researched, evaluated, and tested prior to fielding.

Identifying enterprise systems (ES) that will interact and exchange data with the UTACC system is critical to achieve integration. ESs typically consist of legacy, custom, commercial-of-the-shelf (COTS), and proprietary software [51]. Identifying and planning the integration between UTACC and ES will be challenging. Information such as transfer protocols, data formats, schema, and content is essential in enabling collaboration between systems [51].

The most dangerous threat possibility is the UTACC system being incompatible with other equipment and enterprise systems which are already operational or being fielded by the Marine Corps. The inability to integrate with other systems will lead to the system being deemed ineffective by Marines. An example would be UTACC not integrating with an intelligence system that might utilize data from UTACC to develop the enemy situation.

The most likely threat impact will be that the UTACC may not initially integrate with systems not specifically identified in the requirements document. The UTACC system will be modified during follow-on upgrades that enable compatibility with these initially unidentifed systems. An example is the UTACC system failing to collaborate with a newly acquired handheld device procured by the Marine Corps. The failure might occur due to a transfer protocol, which would be identified and corrected via an upgrade during the operational and testing phase of development.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- When the UTACC system is designed, developed, and employed.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- Network access is a requirement for the UTACC system.
- Each component of the UTACC system will be networked to facilitate data sharing.
- The UTACC system will be required to integrate and share information with other enterprise systems.

SECURITY CONTROLS

- Non-technical Controls
    - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
    - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
    - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
    - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
    - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
    - Continue development of the UTACC concept of operations.
    - Conduct extensive testing and evaluation with operational units.
    - Require vendors to integrate UTACC with current and planned programs of record.
    - Procure government owned and operated software instead of vendor

owned and operated.
    - Use a model driven development approach that produces end points that enable easier integration with other systems.
- Technical Controls
    - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.
    - Utilize commonly used programming languages and standards.
    - Implement standardized data format with identified systems.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX Q. AUTONOMOUS SOFTWARE

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Autonomous Software

THREAT SUMMARY

The UTACC system is intended to be semi-autonomous, allowing partial control to a human user. The autonomy software, however, possesses certain inherent threats that must be addressed and mitigated. Moving to a higher level of autonomous technology is challenging for the DOD because autonomous systems are primarily a software endeavor which is a shift away from the typical DOD hardware-centric development and acquisition process [53]. Autonomous software has the potential to be manipulated by our enemies.

The UTACC concept of operations places the system with the enemy, which possibly gives the enemy access to the system. The UTACC system concept of operations is far more complex than current DOD unmanned systems. Currently autonomous software is most commonly employed on unmanned aerial vehicles (UAV). UAVs are not easily accessible by enemy forces. When the UTACC system is employed on the ground, the enemy may be able to manipulate the sensors to cause the UTACC system to act incorrectly, or manipulate the software to cause damage to the system or injure personnel. In recent years, autonomy as an aspect of diverse systems beyond DOD applications has been targeted by viruses which caused significant damage to hardware and software [54].

Although the system software or hardware that enable HMI have not been developed there are many technological risks involved with this endeavor. The HMI will mostly be comprised of software code that will enable UTACC to integrate into and communicate with the reconnaissance team. Current semi-autonomous aerial vehicles are operated by Marines whose sole purpose is to remotely fly the aerial vehicle. A reconnaissance team does not possess the time or manpower to constantly operate a multi-agent robotic system like UTACC. Unlike current unmanned systems interaction, the UTACC HMI software will be loaded on system components that are co-located with the enemy, which requires security functions to recognize authorized and unauthorized users.

The most dangerous possible threat would be the enemy discovering a limitation or fault in the autonomous software and using the system against friendly troops or causing it to damage itself. For instance UTACC might not recognize the enemy fighters as a threat. The enemy fighters could then make contact with the UTACC system and modify the software or code to attack friendly forces or itself.

The most likely threat permutation would be the enemy discovering the Tactics Techniques and Procedures (TTPs) of the UTACC system and using the knowledge of the procedures to nullify the capabilities gained from the autonomy of the system. An example would be if the system does not operate optimally during heavy rains, the enemy

could conduct operations at this time.

IMPACTS TO THE CIA TRIAD

- This is a threat that could affect confidentiality, integrity, and availability.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing security for the system, unless man-in-the-loop weapon systems are implemented.
- The system will require some form of physical security to protect cryptographic material and keys.
- Network access is a requirement for the UTACC system.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- Each component of the UTACC system will be networked to facilitate data sharing.

SECURITY CONTROLS

- Non-technical Controls
    - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
    - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
    - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
    - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
    - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security

- Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
- Continue development of the UTACC concept of operations.
- Conduct extensive testing and evaluation with operational units.
- Research approaches used by other weapons and information systems.

- Technical Controls
  - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.
  - Implement cryptographic solutions:
    - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
    - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
  - Implement access controls through authentication (Login Information, Passwords, and Biometrics).
  - Implement port security for all external hardware connections (RG-45 ethernet) to prevent unauthorized hardwire access to system components and information.
  - Implement access control through privileges (System administrators, users, etc).
  - Implement a “two person rule” for system administrators to reduce errors and tampering.
  - Research and employ tamper resistant technology.
  - Implement a remote zeroing capability of software, data, and cryptographic material.
  - Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX R. UNENCRYPTED C2 AND DATA LINKS

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Unencrypted Command and Control (C2) and Data Links

THREAT SUMMARY

Unencrypted Command and Control (C2) and data links are frequencies used to pass important information without utilizing encryption techniques. Current Marine Corps Unmanned Aerial Systems (UAS) utilize unencrypted C2 and data links [38]. While these usage patterns might suggest that communication links are safe, in fact they allow an enemy access to exploit myriad vulnerabilities, including eavesdropping, masquerading and virus insertion into our systems. The UTACC system could be more effective than our current unmanned systems by employing encryption techniques to protect C2 and data links.

The most dangerous threat permutation would be the UTACC system being employed and a virus infecting the network through an unencrypted C2 link. An example would be the enemy eavesdropping on an unencrypted C2 link, then masquerading an IP address of the UTACC system and uploading a virus, which impacts the entire network.

The most likely threat impact would be the enemy receiving an unencrypted data feed from the UTACC system at the same time as friendly forces. An example would be that the enemy constructs a receiver that is tunable to the frequency of the data link and is viewing the data stream at the same time as the Marines employing the system.

IMPACTS TO THE CIA TRIAD

- This threat if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- Network access is a requirement for the UTACC system.
- The system has to be able to be left behind in the event of an emergency or loss of life.

- Each component of the UTACC system will be networked to facilitate data sharing.
- Eavesdropping will happen regardless and this threat must be mitigated.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
  - Continue development of the UTACC concept of operations.
  - Conduct extensive testing and evaluation with operational units.
  - Research approaches used by other weapons and information systems.
  - Conduct extensive research of the electromagnetic (EM) spectrum; identify frequency bandwidth requirements of the system, identify portions of the EM spectrum available for use, identify enough EM spectrum to facilitate frequency hopping to mitigate jamming.
  - Coordinate with USMC and DOD frequency management officials to ensure frequency availability.
  - Research the utilization of cognitive radios that seek open spectrum and ensure they are in compliance with USMC COMSEC procedures and the USMC and DOD frequency management policies.
- Technical Controls
  - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.
  - Employ a fully autonomous get home control mode of operation (Shadow UAS).
  - Implement redundant and encrypted C2 and data links spread across the EM spectrum.
  - Implement independent UGV and UAV operations to mitigate the effects if one portion of the UTACC system is jammed.

APPENDIX S. CONTROLLED CRYPTOGRAPHIC ITEM EMPLOYMENT ONBOARD AN AUTONOMOUS SYSTEM

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology	Controlled Cryptographic Items (CCI) Employment Onboard an Autonomous System

THREAT SUMMARY

Controlled Cryptographic Items (CCI) are secure telecommunications or information-handling equipment, or associated cryptographic components that are controlled by the COMSEC Material Control System [55]. Current unmanned systems have a requirement to employ CCI to complete missions which could pose a significant risk to operations and security. The UTACC system will have similar requirements to current unmanned systems and should plan to have CCI onboard during operations. In 2012, a UAV crashed in Afghanistan; it had three CCI items onboard that had to be located, recovered and emptied of cryptographic keys. The Electronic Key Management System (EKMS)-1B sets the policies for issuing, accounting, handling, safeguarding, and disposing of COMSEC material and the policies relating to the application of COMSEC material [55]. Another concern is the cryptographic rollover timeline and how UTACC will conduct a rollover while in the field operating autonomously. If a wireless cryptographic rollover is conducted, this increases the risk of having the keys compromised by enemies. The UTACC system will be expected to maintain the practices and procedures seen in the EKMS 1B to employ COMSEC and meet the standards outlined in the EKMS 1B.

The most dangerous threat permutation would be the enemy discovering our cryptographic keys and utilizing them to gain access to encrypted networks, data, and information. An example would be that the UTACC system endures a malfunction and the UAV or UGV becomes inoperable, giving the enemy access to the cryptology or controlled cryptographic items. The enemy would now be able to reverse engineer the technology to capture over-the-air transfers of keys.

The most likely threat impact would be that the UTACC system has to disengage from an ongoing operation to conduct a cryptographic material rollover. An example would be the UTACC is being employed by a unit to locate a High Value Target (HVT) and at midnight the UTACC has to perform a cryptographic rollover, which pauses operations.

IMPACTS TO THE CIA TARIAD

- These threats if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The system will require some form of physical security to protect cryptographic material and keys.
- Network access is requirement for the UTACC system.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- Each component of the UTACC system will be networked to facilitate data sharing.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Utilize best common practices of the Internet Engineering Task Force by researching Request for Comments (RFC's) for computer and network security
  - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
  - Continue development of the UTACC concept of operations.
  - Conduct extensive testing and evaluation with operational units.
- Technical Controls
  - Employ mandatory semi-autonomous (man-in-the-loop) modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.

- Implement cryptographic solutions:
  - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
  - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
- Implement access controls through authentication (Login Information, Passwords, and Biometrics).
- Implement access control through privileges (System administrators, users, etc).
- Implement a "two person rule" for system administrators to reduce errors and tampering.
- Research and employ tamper resistant technology.
- Implement a remote zeroing capability of software, data, and cryptographic material.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX T. COST THREAT TO THE UTACC SYSTEM RESEARCH, DEVELOPMENT, AND TESTING

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Cost Threat to the UTACC System Research, Development, and Testing

THREAT SUMMARY

The current fiscally constrained environment of the Marine Corps will hinder or halt the development of the UTACC system. If UTACC is developed using new air/ground vehicles, the cost increase could halt system research and development. The MCWL is currently researching and developing other Unmanned Aerial Vehicles (UAV)/Unmanned Ground Vehicles (UGV) to conduct other missions, which is documented in the MCWL campaign plan [56]. This duplication of manpower and money required to research and develop these similar autonomous systems may cause the UTACC system development to be canceled or postponed. Duplication of capabilities is another cost concern which could lead to the cancellation of UTACC. The UTACC system is being designed to provide intelligence, surveillance, and reconnaissance (ISR) to a squad of reconnaissance Marines [28]. These capabilities are currently being completed by other unmanned systems in the operational forces. The capabilities of the UTACC should exceed that of currently fielded unmanned systems.

The most dangerous threat permutation would be the UTACC system not being developed, because it does not provide a unique and reliable set of capabilities to gain a share of funding.

The most likely threat possibility would be the development of the UTACC systems being slowed due to budgetary reasons, even though some of the components required may already be owned or in testing by the Marine Corps.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- The UTACC system's funding, design, development, and procurement processes.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The system will require some form of physical security to protect cryptographic material and keys.
- Network access is requirement for the UTACC system.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- Each component of the UTACC system will be networked to facilitate data sharing.
- The Statement of Work provided the only mission required of UTACC (ISR).

SECURITY CONTROLS

- Non-technical Controls
    - Current and future DOD and USMC policies, procedures and publications must be analyzed to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
    - Research the possibility of integrating UTACC software and mission sets into current MCWL systems and projects. The UTACC could leverage the cargo (Unmanned Ground Vehicle (UGV) and the Shrike and Stalker Unmanned Aerial Systems (UAS) efforts) as a test bed for the UGV and UAV of portions of the UTACC system.
    - Educate leaders and key decision makers on the UTACC system technology and capabilities.
    - Demonstrate the capabilities of the UTACC to Fleet Marine Force personnel and commands.
        - The UTACC system must validate reliability while highlighting capabilities during demonstrations. Results and conclusions of these demonstrations, plus theses, point papers and briefs should be published by the Marine Corps Warfighting Lab to operational units.
    - Incorporate current operational or program of record unmanned systems into the UTACC system. Marines have familiarity with these systems. Utilizing unmanned aerial systems the Marine Corps has already purchased, like STUAS or Raven UASs. The Marines and decision makers are familiar with this equipment, making the transition easier for the Marines, while showcasing the UTACC system capabilities
    - Continue development of the UTACC concept of operations.
    - Develop and adapt appropriate Measures of Performance (MOP) and Measures of Effectiveness (MOE).

APPENDIX U. AIRSPACE INTEGRATION

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Airspace Integration

THREAT SUMMARY

The procurement and utilization of unmanned systems has increased significantly in recent years. The U.S. had fewer than 10 Predator Unmanned Aerial Vehicles (UAV) in 2001 and the fleet grew to 180 by 2007 [57]. Predator UAVs carried out 2,073 missions from June 2005 until June 2006 [57]. Manned and unmanned aircraft are already taking a large share of the airspace system. UAVs operate either autonomously via onboard computers or sensors or semi-autonomously (with a human in the loop). Fully and semi-autonomous unmanned aerial vehicles have the capability to operate at the same altitudes as manned aviation assets. The seamless integration of UTACC into an already crowded airspace system must occur before UTACC is ever employed in a real world scenario.

Development of UTACC will require an in-depth study of current policies, procedures, and regulations that govern both the military and civilian utilization of the airspace system. The USMC currently utilizes three different types of UAVs. Larger UAVs like the Shadow and STUAS require adherence to the Naval Aviation Training and Operating Procedure Standardization (NATOPS) and must be operated by trained Aerial Vehicle Operators (AVO) and Mission Commanders (MC) who are integrated into the Air Command Element (ACE). Both the Shadow and Small Tactical Unmanned Aerial System (STUAS) UAVs are classified as Group Three UAVs. The Shadow UAV operates between 4,000 and 10,000 feet Above Ground Level (AGL), while the STUAS UAV operates between 1,500 to 5,000 feet AGL [38]. Both the Shadow and STUAS will appear on the Air Tasking Order (ATO) with the operating times and altitude to integrate into the airspace with manned aviation assets [38]. The Shadow and STUAS UAVs are equipped with a transponder enabling positive and procedural control, which requires two way communication with the controlling agency (DASC/FAC) [38]. The smallest UAV operated by the Marine Corps is the Raven which may be a comparable size to the UTACC UAV. Raven UAVs operate at or below 1,200 feet AGL, which is coordinated by the battalion air officer to integrate with rotary wing assets and they do not require a trained MC or AVO to operate [38]. A detailed review of how current UAVs are employed by the Marine Corps will provide the foundation for integration of UTACC. As the UTACC design solidifies and as requirements increase, the size of the UAV will determine who and how the system will be employed. A completely autonomous air vehicle operating in congested airspace above a target or area of interest increases the risk of employing the UTACC system.

The most dangerous variation of this threat would be UTACC being employed in support of a mission along with manned aviation assets. The UAV may be launched, without the knowledge of the aviators and a mid-air collision causes a mishap and destroys the aircraft and possibly kills the crew.

The most likely threat permutation would be the UTACC UAV being grounded due to safety of flight concerns with manned aviation assets. A reconnaissance team does not possess

the resident expertise in airspace integration and will not employ the system if it endangers other airborne assets also supporting their mission.

IMPACT TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- When the UAV portion of the UTACC system is employed in the airspace system.

ASSUMPTIONS

- Federal Aviation Administration, Department of Defense, and specifically the reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The UAV portion of the UTACC system will be grounded if integration is not achieved.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future FAA, DOD, and USMC policies, procedures and publications to determine specific system requirements of the UAV. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the UAV.
  - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit.
  - Ensure integration within the airspace system in both a deployed and non-deployed environment.
- Technical Controls
  - Limit altitude and range of the UAV.
  - Identify UAV size and the equipment required (Identify Friend or Foe).
  - Employ mandatory semi-autonomous modes of operation.
  - Implement Independent UGV and UAV operations.
  - Ensure the UTACC mission planning component includes parameters to ensure integration with manned aviation assets and aviation command and control units.

APPENDIX V. SURFACE SPACE INTEGRATION OF UTACC

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Surface Space Integration of UTACC

THREAT SUMMARY

The procurement and utilization of unmanned ground systems will increase as technological advances occur. Civilian companies, like Torc Robotics, are on the cutting edge of technology in regards to Unmanned Ground Vehicles (UGV), and have developed new ways to ensure the navigation and route selection of these vehicles. The ability to integrate UGVs into high traffic areas such as urban areas, freeways, and into Marine Corps convoys and vehicle formations has not been fully developed and tested because the U.S. military has up to now used UGVs to conduct Explosive Ordnance Disposal (EOD) missions [57].

Surface space integration is key to the success of the UTACC system. The system must keep intervals with manned vehicles, maintain a safe speed, maintain march discipline, and must not become a hindrance to the Marines or the mission [58]. The UGV must be able to discern obstacles and hazards, and be able to identify people as threats and non-threats. It also must prioritize the lives of Marines and civilians above its survival.

The most dangerous threat possibility would be that the UTACC is employed in support of a mission, integrated with manned vehicles, and either injures or kills a Marine or civilian or damages other equipment essential to the mission. An example would be that the UTACC UGV is trying to avoid an obstacle in the road and a Marine or civilian walks into the alternate path. The UGV hits the Marine or civlian, resulting in their death.

The most likely threat scenario is that the UGV portion of the UTACC gets trapped in an urban area due to enemy or obstacles. The UGV will not be recovered and the equipment is lost to the enemy or destroyed. An example would be the UGV making a turn onto a crowded street and being surrounded by people, and unable to turn around; the enemy is able to apprehend the UGV without any engagement.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- When the UGV portion of the UTACC system is employed in any environment.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- The UGV loss is an acceptable loss compared to that of innocent non-combatants and Marines.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC UGV requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the UGV.
  - Classify and protect UTACC system software throughout system life-cycle. Procure and manufacture components from trusted companies.
  - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Ensure integration within the surface space system in both a deployed and non-deployed environment.
  - Extensive research of convoy operations, Standard Operating Procedures (SOP) and Tactics Techniques Procedures (TTP).
  - Continue development of the UTACC concept of operations.
  - Extensive testing and evaluation with operational units.
  - Research lessons learned from the "Google Car" and companies like Torc Robotics.
- Technical Controls
  - Limit speed and range of the UGV in certain environments or situations.
  - Identify size and weight requirements of the UGV
  - Employ mandatory semi-autonomous modes of operation.
  - Implement a remote zeroing capability of software, data, and cryptographic material.
  - Implement independent UGV and UAV operations.

APPENDIX W. HUMAN MACHINE INTERACTION

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Technology/Operations/People	Human Machine Interaction (HMI)

THREAT SUMMARY

Human Machine Interaction (HMI) spans the three threat areas of People, Technology, and Operations and is the linchpin of UTACC. The People aspect of the HMI threat is seen in Appendix D (Attitude Towards Emerging Technologies), the Technology aspect of the HMI threat is seen in Appendix Q (Autonomous Software), and the Operations aspect of HMI will be explained in this template. The HMI software must enable simple and effortless interaction of system command and control (C2) and intelligence, surveillance, and reconnaissance (ISR) mission data. The HMI software is what will operationally enable UTACC to integrate into the reconnaissance team and become a team member. The HMI software development is critical in overcoming potential shortfalls in robot and human teams. The end state of UTACC should be to allow Marines to focus on the mission and not on the controller of an autonomous system.

The HMI software threat to operations is when it fails to provide the operational capabilities outlined initially by the Statement of Work (SOW) between the Naval Postgraduate School (NPS), the Marine Corps Warfighting Lab (MCWL) and the Marines testing the UTACC system. Failing to integrate UTACC at the team level will put the team of Marines at risk. The HMI must significantly minimize the operator interaction over current systems while providing capabilities to accomplish multiple mission sets [28]. Operationally the HMI software must both transmit and receive communication through multiple mediums to truly integrate into a reconnaissance team. Marines on the battlefield communicate with each other in many different and unique methods. UTACC must be adaptable to these different methods of communication and immediately perform actions based on the information received from teammates. The UTACC HMI must also alert and display to team members operationally relevant and timely mission information. The UTACC system will be operating in a dynamic environment in which every situation cannot be foreseen or predicted. The system developers must capture as much operational information about the team employing UTACC to provide a fully assimilated and operationally capable system.

The most dangerous threat impact would be that the UTACC HMI does not reduce operator interation. The system does not improve current HMI and this causes the death of Marines. For instance Marines are employing the system and it requires a significant amount of interaction from a team member. That team member is also responsible for security of a certain area, which is breached because the Marine is focused on UTACC. The enemy identifies and kills the Marines.

The most likely threat permutation would be the UTACC concept of operations is too complex to enable the required level of HMI at this point in time. Research and development continues and allows for technology to advance to a point where the HMI

can be reliably employed on a battlefield.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability, if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- During demonstrations of UTACC that showcase capabilities for potential units.

ASSUMPTIONS

- HMI is not technically mature enough to operate effectively in combat.
- UAV/UGV autonomous operations

SECURITY CONTROLS

- Non-technical Controls
    - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
    - Develop the UTACC system security policies and procedures which meet the requirements of the DOD and USMC. Ensure the UTACC system completes the DIACAP process, which ensures the system meets DOD requirements for IA.
    - Educate leaders and key decision makers on the UTACC system technology and capabilities.
    - Demonstrate the capabilities of the UTACC to Fleet Marine Force personnel and commands.
        - The UTACC system must validate reliability while highlighting capabilities during demonstrations. Results and conclusions of these demonstrations, plus theses, point papers and briefs should be published by the Marine Corps Warfighting Lab to operational units.
    - Incorporate current operational or program of record unmanned systems into the UTACC system. Marines have familiarity with these systems.
    - Research the ability to incorporate current operational or program of record unmanned systems into the UTACC system. Marines have

familiarity with these systems.
    - Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit. This includes pre-deployment training packages.
    - Continue development of the UTACC concept of operations.
    - Conduct extensive testing and evaluation with operational units.
    - Extensive research of the information exchange process and requirements for the UTACC system.
- Technical Controls
    - Employ mandatory semi-autonomous modes of operation, with which Marine Corps personnel are familiar and which they have employed in combat operations.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX X. RECONNAISSANCE TEAM EMPLOYMENT OF UTACC

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Reconnaissance Team Employment of UTACC

THREAT SUMMARY

The proposed operational employment context of the UTACC system with a USMC reconnaissance team may not be the best fit for a system of this size and scope. These teams work well because of their ability to conduct reconnaissance of the enemy and the terrain for future operations, while remaining undetected and uncompromised [59]. The UTACC system adds a significant physical footprint to a small team that is used to operating with limited equipment, connectivity and in austere conditions on a mission that may take a significant amount of time. Some insertions/extractions must be timed to coincide with particular lighting, weather, or tidal conditions [59]. Operating with UTACC, the reconnaissance team has to accomplish the location, camouflage, and concealment of themselves and the system. Reconnaissance teams rely on stealthy maneuvering, timely and accurate intelligence reporting, and information obtained without enemy knowledge [59]. To maximize effectiveness, reconnaissance units must be able to approach the enemy, the Named Areas of Interest (NAI), or other objectives uncompromised [59]. Remaining uncompromised and in advantageous positions while conducting reconnaissance missions will be increasingly difficult with the physical components of UTACC.

The most dangerous threat permutation would be discovery of the system through observation of the Unmanned Aerial Vehicle (UAV), Unmanned Ground Vehicle (UGV) or the digital footprint of UTACC which leads to the discovery of the team. An example would be that the enemy discovers the UGV/UAV which leads to the discovery and kill/ capture of the reconaissance team and ultimate mission failure.

The most likely threat possibility would be discovery of the system which puts the mission at risk. It is the mission of the reconnaissance team to locate the enemy and establish patterns of behavior. If the UAV or UGV is seen or heard the enemy will change their patterns which is the mission of the reconnaissance team to locate and pattern the enemy.

IMPACTS TO THE CIA TRIAD

- This threat if not mitigated will impact confidentiality, integrity, and availability of the UTACC system.

IMPACTS TO UTACC
VULNERABILITY ANALYSIS • When the UTACC system is employed in an operational environment by a reconnaissance team.
ASSUMPTIONS • Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member. • The system has to be able to be left behind in the event of an emergency or loss of life. • The Reconnaissance team is not providing security for the system, unless man-in-the-loop weapon systems are implemented. • The UTACC system will increase the physical and digital footprint of a reconnaissance team.
SECURITY CONTROLS • Non-technical Controls o Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit. o Ensure integration within the surface space system in both a deployed and non-deployed environment. o Extensive research of convoy operations, Standard Operating Procedures (SOP) and Tactics Techniques Procedures (TTP). o Continue development of the UTACC concept of operations. o Extensive testing and evaluation with operational units to determine best fit for the USMC. o Research power generation methods other than traditional methods to increase operational endurance. o Research and employ camouflage and concealment technologies for the UTACC system to employ. o Research technologies to maintain light discipline during nighttime operations. o Research and employ noise dampening technology. o Research emerging cloaking technologies. • Technical Controls o Identify size and weight requirements of the UGV o Implement independent UGV and UAV operations. o Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations. o Implement cryptographic solutions: ▪ Asymmetric (Public key) cryptography is based on the use of key

pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
        - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
    - Implement access control through authentication (Login Information, Passwords, and Biometrics).
    - Implement access control through privileges (System administrators, users, etc).
    - Implement a "two person rule" for system administrators to reduce errors and tampering.
    - Research and employ tamper resistant technology.
    - Implement a remote zeroing capability of software, data, and cryptographic material.
    - Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX Y. SURVIVABILITY OF THE SYSTEM FROM ENEMY WEAPONRY

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Survivability of the System from Enemy Weaponry

THREAT SUMMARY

The enemy has a wide range of weapons from small arms to precision missiles. The UTACC system will be targeted by these weapons and must meet military standards that protect equipment from this threat. Currently, Unmanned Aerial Vehicles (UAV) are targeted primarily by enemy small arms fire and anti-air artillery weapons [38]. The UTACC UAV will be subjected to these same weapons, but the Unmanned Ground Vehicle (UGV) will be the most vulnerable component because it is geographically co-located with enemy forces. Unmanned Aerial Systems (UAS) survivability is achieved by reducing the vulnerability of the total system to include the ground control systems, vehicles, and the Marines that operate and maintain the systems [38]. These current UASs have ground components that are not employed in the same locations or with the same mission as the UTACC UGV. UTAAC will require some type of physical and connective security measures to protect and control a degraded UTACC system or components. UTACC must implement both strategies to protect and prevent affects from enemy weaponry. Steps to protect UTACC from enemy weaponry include adding a type of armor that protects the system. Measures to prevent UTACC from being targeted by enemy weaponry include concealment and camouflage to system components.

The most dangerous threat permutation would be the absolute destruction of the UTACC system by an explosion or direct fire from enemy weapons. An example of this would be the UAV being targeted by an anti-air missile or the UGV hitting an improvised explosive device (IED). If the UTACC is profoundly disabled and the oboard informaiton cannot be deleted remotely, the information may be extracted and used by the enemy. The enemy would be able to replicate and reverse engineer the technology which would greatly impact future employment of the system.

The most likely threat impact would be the system coming into contact with enemy forces and certain components being damaged. An example of this would be the UGV/UAV being engaged by enemy forces and losing a sensor and a communications link. This loss would degrade the UTACC system but would not result in a complete system failure.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- UTACC is vulnerable to this threat during the design, development, and employment stages when a malicious actor has the ability to access the system.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- The Reconnaissance team is not providing security for the system, unless man-in-the-loop weapon systems are implemented.

SECURITY CONTROLS

- Non-technical Controls
  - Training pipeline for leaders, planners, operators, and maintainers to support the UTACC system employment by a USMC unit.
  - Extensive research of convoy operations, Standard Operating Procedures (SOP) and Tactics Techniques Procedures (TTP).
  - Continue development of the UTACC concept of operations.
  - Extensive testing with operational units to determine best fit for the USMC.
  - Research and employ technologies to provide protection of critical UTACC system components (armor).
  - Research power generation methods other than traditional methods to increase operational endurance.
  - Research and employ camouflage and concealment technologies for the UTACC system to employ.
  - Research and employ technologies to maintain light discipline during nighttime operations.
  - Research and employ noise dampening technology.
  - Research emerging cloaking technologies.
- Technical Controls
  - Identify size and weight requirements of the UGV
  - Employ independent UGV and UAV operations.
  - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.
  - Implement cryptographic Solutions
    - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires

significant infrastructure [36].
        - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
    - Implement access control through authentication (Login Information, Passwords, and Biometrics).
    - Implement access control through privileges (System administrators, users, etc).
    - Implement a "two person rule" for system administrators to reduce errors and tampering.
    - Implement a remote zeroing capability of software, data, and cryptographic material.
    - Implement independent UGV and UAV operations.
    - Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).
    - Research and employ tamper resistant technology.
    - Implement redundant and encrypted C2 and data links spread across the EM spectrum.
    - Implement redundant sensors.
    - Employ Defense Electronic Counter-Measures (DECM) (Chaff, Flare, Radar).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX Z. ENVIRONMENTAL THREATS

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Environmental Threats

THREAT SUMMARY

Current Marine Corps Unmanned Aerial Systems (UAS) cannot effectively operate in the rain and provide limited operational capabilities in hot, sandy, or dusty environments. The Shadow UAS cannot be operated in rain; however, the Small Tactical UAS (STUAS) can operate in light rain [38]. UTACC must overcome the environmental limitations of current Intelligence Surveillance and Reconnaissance (ISR) assets. Limitations of current UASs include: the inability to operate in heavy rain and excessive heat, require manual switching between day electro-optical (EO) and night Infrared (IR) sensors, and are vulnerable to space weather effects, low cloud decks, sea state/sea spray, and high altitude environments [38].

Per the Statement of Work (SOW) between the Naval Postgraduate School (NPS) and the Marine Corps Warfighting Lab (MCWL) the system must be able to withstand a wind speed of 15 knots minimum, operate in sandy and dusty environments (MIL-STD-810G, 510.6), and rain (MIL-STD 810G, 506.5) [28]. These requirements provide initial specifications but must be refined to include the full spectrum of environmental possibilities in which UTACC will be expected to operate.

The most dangerous environmental threat impact would be that UTACC system or its components are damaged, destroyed, cause a mishap or are lost due to environmental conditions. For example the UTACC Unmanned Aerial Vehicle might be conducting a mission and an unexpected thunderstorm arises in the operational area. The UAV crashes into a populated area and kills innocent civilians or friendly forces.

The most likely environmental threat possibility is that weather negates the capabilities of a specific system component, like the UAV. For instance, heavy rains and cloud cover prevent the UAV from launching and is not employed. The Unmanned Ground Vehicle (UGV) is still able to provide limited capabilities and is employed independently of the UAV. The Marines will overcome the limitations of the air vehicle, but will have less faith in the system as a whole.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC
VULNERABILITY ANALYSIS • When the UTACC system is employed in any environment.
ASSUMPTIONS • Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member. • The system has to be able to be left behind in the event of an emergency or loss of life. • Environmental effects will limit capabilities provided by portions of or the entire UTACC system. • The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Establish training pipeline for leaders, planners, maintainers, and operators to support the UTACC system employment by a USMC unit.
  - Achieve MIL-STD for electrical wiring and electronic components.
  - Adhere to USMC Communications Security (COMSEC) standards and policies which includes physical, cryptographic, transmission, and emission security.
  - Continue development of the UTACC concept of operations.
  - Extensive system testing to determine limitations with regards to environmental effects.
  - Achieve the minimum MIL-STD referenced for rain, wind, dusty environments.
  - Research technologies that enable waterproofing of UTACC (Nano coatings).
  - Establish corrosion prevention requirements and maintenance procedures.
  - Research and conduct a cost benefit analysis of employing low cost throw-away unmanned vehicles.
- Technical Controls
  - Implement independent UGV and UAV operations.
  - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.
  - Research and employ tamper resistant technology.
  - Research and employ ruggedized components that protect against environmental effects (rain, wind, sand)
  - Implement a remote zeroing capability of software, data, and cryptographic material.
  - Implement redundant and encrypted C2 and data links spread across the EM spectrum.
  - Implement redundant sensors.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX AA. TERRAIN

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Terrain

THREAT SUMMARY

The UTACC system must be functional in most terrains to provide sustained capabilities to Marines. The Statement of Work (SOW) specifies high and low altitudes, open desert, thick vegetation and canopy cover, rocky cliffs and mountainous terrain, as well as urban environments [28]. Expeditionary Force 21 states that the ability to conduct amphibious assaults on littoral terrain such as islands, archipelagos, straits, or shorelines for future operations is imperative [60]. These requirements provide initial specifications but must be refined to include any terrain in which UTACC will be expected to operate. The UTACC system design must be able to operate in all the above terrains to be considered an asset to the Marine Corps and Future Maritime Operations (FMO).

Different altitudes and terrains introduce different challenges to line of sight (LOS) communications links, maneuverability, speed, and visibility from both the Unmanned Aerial Vehicle (UAV) and Unmanned Ground Vehicle (UGV) perspectives. Speed and surprise are key tenets in "maneuver warfare," which is the basis for Marine Corps doctrine [61]. For this system to provide an increased capability to the warfighter it must overcome the limitations of assets that currently conduct Intelligence, Surveillance, and Reconnaissance (ISR) missions. With current unmanned systems, terrain affects launch and recovery sites. The Shadow Unmanned Aerial System (UAS) requires a runway for operations and the Small Tactical UAS (STUAS) requires a landing zone (LZ) for launch and recovery operations [38]. These requirements slow operational tempo and this is an area where UTACC could provide unique capabilities to support maneuver warfare.

The most dangerous threat impact of operating on challenging terrain is that the UTACC UGV becomes immobilized and is unable to provide a platform for UAV operations or provide ground-based ISR. For instance the UGV could roll over on mountainous terrain. The UAV then cannot take off or land from the UGV, causing mission failure. The system in this scenario provides no capabilities to the team, and at this point is a liability.

The most likely threat possibility would be that the terrain negatively impacts the system, but not the mission itself. An example would be the UAV is not operational due to mountainous terrain impacting communication and data links, but the UGV can still effectively complete its portion of the mission. The Marines will overcome the limitations of the air vehicle, but will have less faith in the system and have far less situational awareness than if the system was fully functional in this terrain.

INMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- When the UTACC system is employed in any environment.

ASSUMPTIONS

- Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member.
- The system has to be able to be left behind in the event of an emergency or loss of life.
- Portions of the UTACC system will be left unattended if it cannot traverse the terrain.
- Terrain will limit UTACC system capabilities.
- The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD and USMC policies, procedures and publications to determine specific UTACC system requirements. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system.
  - Establish training pipeline for leaders, planners, maintainers, and operators to support the UTACC system employment by a USMC unit.
  - Continue development of the UTACC concept of operations.
  - Conduct extensive testing and evaluation to determine limitations with regards to terrain.
  - Achieve the minimum requirements for traverse ability (incline, altitude, etc).
- Technical Controls
  - Implement independent UGV and UAV operations.
  - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.
  - Research and employ tamper resistant technology.
  - Research and employ ruggedized components that protect against environmental effects (rain, wind, sand)
  - Implement a remote zeroing capability of software, data, and cryptographic material.
  - Implement redundant and encrypted C2 and data links spread across the EM spectrum.
  - Implement redundant sensors.
  - Ensure the Mission Planning software accounts for terrain limitations of the system.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX BB. SHIPBOARD OPERATIONS

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Shipboard Operations

THREAT SUMMARY

Future Maritime Operations (FMO) will be the primary focus of concept-based experimentation in FY2015 and if UTACC cannot integrate into this environment it will not be fully researched and developed [56]. An example of FMO integration would be enhancing Command and Control (C2) enablers and ship-to-shore connectors, which are areas of interest in the MCWL campaign plan [56]. Expeditionary Force 21 predicts that the future operations of the Marine Corps will be in the littorals and missions are likely to involve maritime operations [60].

The naval platform from which UTACC will be based and operated has unique physical and environmental characteristics. Depending on the type of operations required of the unit employing the UTACC system, the Unmanned Ground Vehicle (UGV) and Unmanned Aerial Vehicle (UAV) must be able to perform certain functions aboard the ship in order to be effective. The UGV might be required to move either autonomously or semi-autonomously onboard the ship to enable embarkation and de-embarkation of the system. The UAV could possibly conduct missions from the ship and would require takeoff and recovery operations from a moving platform. Additionally, maintenance must be performed within the confined spaces of a ship. The shipboard environment also introduces salt water and extreme temperatures, which negatively impacts communication and autonomous systems [38].

A network component threat exists when connecting a Marine Corps system into the Navy's shipboard communication architecture and electromagnetic (EM) spectrum. The RQ-7 Shadow UAS and RQ-11 Raven UAS are not shipboard capable, which severely impacts ship-to–shore capabilities [38]. For UTACC to be successful it must integrate into shipboard operations.

The most dangerous threat impact of shipboard operations is the incompatibility of systems and the inability of the system to operate on the ship. An example of this would be the UGV not being able to move itself in the well deck or onto a Landing Craft Air Cushion (LCAC) when needed due to the ship moving underneath it. Additionally, the incompatibility of systems would leave the unit commander without a communication link to the UTACC system from the Landing Forces Operations Center (LFOC) for common full motion video feeds.

The most likely threat is limiting the capability of the UTACC system. An example of this is the inability of the UAV to take off and land on a ship, due to winds, frequency confliction with the Navy, or UAV / UGV design. Ship to shore operations are extremely complex and if the UTACC is to be successful in the Marine Corps it must provide the ability to assist in power projection from ship-to-shore.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC

VULNERABILITY ANALYSIS

- When the UTACC system is employed onboard ship or requires systems integration with Navy communications networks.

ASSUMPTIONS

- Changing anything on any Navy ship to support the UTACC system is expensive and timely.

SECURITY CONTROLS

- Non-technical Controls
  - Analyze current and future DOD, DoN, USMC policies, procedures and publications to determine specific system requirements of UTACC. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of UTACC.
  - Establish training pipeline for leaders, planners, maintainers, and operators to support the UTACC system employment by a USMC unit.
  - Continue development of the UTACC concept of operations.
  - Conduct testing and integration during shipboard operations and networks (ISR, SATCOM, UHF, EHF).
  - Research and testing of UAV and UGV operations from a moving ship (launch, recovery, and embarkation)
  - Achieve MIL-SPEC wiring and communications circuits to avoid issues from salt water and extreme temperatures.
  - Research technologies that enable waterproofing of UTACC (Nano coatings).
- Technical Controls
  - Independent UGV and UAV operations.
  - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.
  - Establish simplified maintenance procedures that are enabled while embarked on a ship (space constraints).
  - Implement independent UGV and UAV operations.
  - Research and employ tamper resistant technology.
  - Research and employ ruggedized components that protect against environmental effects (rain, wind, sand, salt water)
  - Implement a remote zeroing capability of software, data, and cryptographic material.
  - Implement redundant and encrypted C2 and data links spread across the EM spectrum.
  - Implement redundant sensors.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX CC. OPERATIONAL ENDURANCE

THREAT AREA (PEOPLE, TECHNOLOGY, OPERATIONS)	**THREAT**
Operations	Operational Endurance

THREAT SUMMARY

Reconnaissance teams conduct both mounted and dismounted operations. Though it is a goal of UTACC to be integrated into dismounted operations it will be easier for UTACC to be integrated into mounted operations. Ground mobility assets enable reconnaissance teams to conduct reconnaissance missions of extended range and duration [59]. The UTACC system could be more easily integrated into mounted operations due to organic logistical support. The UTACC system could provide additional transport and organic intelligence, surveillance, reconnaissance (ISR) capabilities to the team.

A reconnaissance team can conduct dismounted operations for a minimum of ninety-six hours with little or no external direction or support while maintaining themselves and their equipment [59]. Their equipment and supplies include only what can be carried on foot while operating dismounted [59]. Reconnaissance Marines will not have support capabilities, such as generators, extra batteries, or fuel, during missions. In order to integrate into dismounted operations the UTACC system must be self-sustaining for the minimum ninety-six hour time period. UTACC must be self-contained and may be forced to provide its own battery storage, power generation capabilities (solar power), and fuel. Another concern of the UTACC system in this environment is system maintenance. The UTACC system needs to be simply designed, so that a team of Marines in the field can maintain it with minimal equipment.

The most dangerous threat permutation would be the UTACC system being unable to operate for the minimum 96 hour time period for dismounted operations, without external logistical support. This would lead to the team not employing the UTACC system for dismounted operations which is a goal of UTACC.

The most likely threat impact is that the UTACC system would only be operable for a limited time with minimal mantainance or significant recharging. An example of this would be UTACC being operational for 2 out of the 4 days needed for a mission. After those 2 days the team would either need to evacuate or hide the UTACC system. If the system is not operational the Marines would have to manually move the system to the extraction point or shut the system down to save enough power and fuel to retrograde the system. This would minimize the capability provided by the UTACC system.

IMPACTS TO THE CIA TRIAD

- This is a threat to availability; if the threat is not mitigated the system will not be available for use in operations.

IMPACTS TO UTACC
VULNERABILITY ANALYSIS • When the UTACC system is employed in an operational environment by a reconnaissance team.
ASSUMPTIONS • Reconnaissance community will not change their SOP's, doctrine, and best common practices to enable the utilization of poor technology that cannot adapt to the standards of an operational team member. • The system has to be able to be left behind in the event of an emergency or loss of life. • The Reconnaissance team is not providing constant security for the system, unless man-in-the-loop weapon systems are implemented. • The team will not carry excessive amounts of additional gear to support the UTACC system. • The UTACC system will increase the physical and digital footprint of a reconnaissance team.
SECURITY CONTROLS • Non-technical Controls o Current and future DOD and USMC policies, procedures and publications must be analyzed to determine specific system requirements of UTACC. Requirements lead to the development of system specifications which will drive operational employment, training, and integration of the system. o Establish training pipeline for leaders, planners, and operators to support the UTACC system employment by a USMC unit. o Ensure integration within the surface space system in both a deployed and non-deployed environment. o Extensive research of convoy operations, Standard Operating Procedures (SOP) and Tactics Techniques Procedures (TTP). o Continue development of the UTACC concept of operations. o Extensive testing and evaluation with operational units to determine best fit for the USMC. o Research power generation methods other than traditional methods to increase operational endurance. o Research and employ camouflage and concealment technologies for the UTACC system to employ. o Research technologies to maintain light discipline during nighttime operations. o Research and employ noise dampening technology. o Research emerging cloaking technologies. o Research the mission sets that enable UGV employment.

- Research the possibility of an unmanned re-supply concept for UTACC to increase UTACC system range.

- Technical Controls
  - Identify size and weight requirements of the UGV
  - Implement independent UGV and UAV operations.
  - Employ mandatory semi-autonomous modes of operation, which Marine Corps personnel are familiar with and have employed in combat operations.
  - Implement cryptographic Solutions
    - Asymmetric (Public key) cryptography is based on the use of key pairs (public and private) and only the private key must be kept secret [35]. Public key cryptology is expensive and requires significant infrastructure [36].
    - Symmetric (Secret key) cryptography is characterized by the fact that the same key is used to encrypt and decrypt data [35]. The key distribution issues are present within symmetric cryptography [36].
  - Implement access control through authentication (Login Information, Passwords, and Biometrics).
  - Implement access control through privileges (System administrators, users, etc).
  - Implement a "two person rule" for system administrators to reduce errors and tampering.
  - Research and employ tamper resistant technology.
  - Research and employ ruggedized components that protect against environmental effects (rain, wind, sand, salt water)
  - Implement a remote zeroing capability of software, data, and cryptographic material.
  - Implement redundant and encrypted C2 and data links spread across the EM spectrum.
  - Implement redundant sensors.
  - Ensure the UTACC network communication links are separated from the USMC communication architecture through best practices (boundary, firewall, router access control lists, Virtual Local Area Networks (VLANS)).
  - Onboard storage for batteries, fuel, maintenance equipment.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] United States Navy. (1995). *NDP 6: Naval Command and Control*. [Ebrary version]. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/ a304321.pdf

[2] Whitsett, J. W. "Security of the user centric cloud." M.S. Thesis, Dept. Cyber Academic Group, Naval Postgraduate School, Monterey, Ca, March 2014.

[3] *DOD Information Assurance Certification and Accreditation Process*, DOD Instruction 8510.01, Department of Defense, Washington, D.C., 2014.

[4] *Marine Corps Order 5400.52*, Department of the Navy, United States Marine Corps, Washington, D.C., 2010.

[5] IASO Terminology. (n.d.). United States Army. [Online]. Available: https://ia.signal.army.mil/IAF/IASOTerminology.asp. Accessed Jan. 12, 2015.

[6] *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009, Committee on National Security Systems. Apr. 26, 2010. [Online]. Available: http://www.ncix.gov/publications/policy/docs/ CNSSI_4009.pdf.

[7] US Code, Title 44, Section 3542, 2006.

[8] NSA. (n.d.) Defense in Depth. [Online]. Available: https://www.nsa.gov/ ia/_files/support/defenseindepth.pdf

[9] B. Guttman and E. Roback.(1995, Oct.). NIST SP 800–12: An Introduction to Computer Security: The NIST Handbook. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://csrc.nist.gov /publications/nistpubs/800-12/handbook.pdf.

[10] Department of Defense. (2002, Oct. 24). DOD Directive 8500.01E: Information Assurance. [Online]. Available: http://www.dtic.mil/whs /directives/corres/pdf/850001p.pdf.

[11] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, Upper Saddle River, NJ: Pearson Prentice Hall, 2008.

[12] Computer Security Division. (2004, Feb.). FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://csrc.nist.gov/publications/ fips/fips199/FIPS-PUB-199-final.pdf.

[13] S. Ram and J. Liu, “Understanding the Semantics of Data Provenance to Support Active Conceptual Modeling,” in Active Conceptual Modeling of Learning, Berlin, Springer, 2007, pp. 17–29.

[14] Computer Security Division. (2011, Mar.). NIST Special Publication 800–39: Managing Information Security Risk. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://csrc.nist. gov/ publications/nistpubs/800-39/SP800-39-final.pdf.

[15] Computer Security Division. (2012, Sep.). NIST Special Publication 800–30: Guide for Conducting Risk Assessments, Rev 1. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[16] Computer Security Division. (2013, Apr.). NIST Special Publication 800–53: Security and Privacy Controls for Federal Information Systems, Rev 4. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/ NIST.SP.800-53r4.pdf.

[17] Computer Security Division. (2010, Feb.). NIST Special Publication 800–37: Guide for Applying the Risk Management Framework to Federal Information Systems, Rev 1. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://csrc.nist.gov/ publications/ nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

[18] Computer Security Division. (2006, Mar.). FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[19] Committee on National Security Systems. (2012, Mar. 15). CNSS Instruction 1253: Security Categorization and Control Selection for National Security Systems, Ver 2. [Online]. Available: http://www.sandia.gov/FSO/PDF/ flowdown/Final_CNSSI_1253.pdf.

[20] Department of the Navy. (2008). DOD Information Assurance Certification and Accreditation Process (DIACAP) Handbook. V 1.0

[21] D. W. Gage. (1990) *Security Considerations for Autonomous Robots*. Autonomous Systems Branch, Code 442, Naval Ocean Systems Center, San Diego, Ca.

[22] Department of Defense. (2011). DOD Strategy for Operating in Cyberspace. [Online]. Available: http://www.defense.gov/news/d20110714cyber.pdf

[23] "Network Security Core Principles," class notes for Network Security, Dept. of Computer Science, Naval Postgraduate School, Monterey, Ca, summer 2014.

[24] United States Marine Corps, *MCDP 6: Command and Control*. Washington, D.C., Department of the Navy, 1996

[25] R. Richardson, *CSI Computer Security and Crime Survey*. New York: Computer Science Institute, 2010/2011.

[26] Technology. (2015). *Oxford Dictionary of English.* [Online]. Available: http://www.oxforddictionaries.com/us/definition/american_english/technology

[27] Information Technology. (2015). *Oxford Dictionary of English.* [Online]. Available:http://www.oxforddictionaries.com/us/definition/american_english/information-technology?q=information+technology

[28] Fiscal Year 2014 Statement of Work (FY14 SOW). (2014). *Statement of Work for Naval Postgraduate School Concept of Operations Development Support to the Marine Corps Warfighting Laboratory Unmanned Tactical Autonomous Control and Collaboration Project*.

[29] United States Marine Corps, *MCWP 3-40.3: MAGTF Communication Systems.* Washington, D.C., Department of the Navy. 1996.

[30] Cyberthreat. (2015). *Oxford Dictionary of English.* [Online]. Available: http://www.oxforddictionaries.com/us/definition/american_english/cyberthreat

[31] Computer Security Division. (2002, Jul.). NIST Special Publication 800–30: Guide for Conducting Risk Assessments. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[32] University Information Technology Services. (2012). Threat Table. University of Connecticut. [Online]. Available: http://uits.uconn.edu/wp-content/uploads/sites/427/2012/04/ctref.doc

[33] Cole, E., and Ring, S. (2005). *Insider Threat : Protecting Enterprise from Sabotage Spying and Theft.* Rockland, MA, Syngress Publishing. [Online]. Available: http://www.ebrary.com

[34] EC Council, *Ethical Hacking and Countermeasures*, Ver 8. Albuquerque, NM: EC Council, 2011.

[35] Douligeris, C. and Serpanos, D. (2007). PKI Systems: Chapter 23 Ed. 1. Wiley-IEEE Press. [Online] Available: http://ieeexplore.ieee.org.libproxy.nps.edu/xpl/ebooks/bookPdfWithBanner.jsp?fileName=5237825.pdf&bkn=5237765&pdfType=chapter

[36] "Cryptology principles," class notes for Network Security, Dept. of Computer Science, Naval Postgraduate School, Monterey, Ca, summer 2014.

[37] "E-authentication" class notes for Network Security, Dept. of Computer Science, Naval Postgraduate School, Monterey, Ca, summer 2014.

[38] United States Marine Corps, *MCWP 3–42.1: Unmanned Aerial Systems Operations DRAFT*. Quantico, VA: Marine Corps Combat Development Command. 2014

[39] C. Meinel and H. Sach. (2012). Internet-Working. New York: Springer.

[40] V. Groom and C. Nass. (2007). *Can Robots be Teammates?* Stanford, Ca: John Benjamins Publishing Company, Stanford University.

[41] Ad Hoc Autonomy Levels for Unmanned Systems Working Group Participants. (2008, Oct.). NIST Special Publication 1011-I-2.0: Autonomy Levels for Unmanned Systems (ALFUS) Framework, Vol 1. National Institute of Standards and Technology, Gaithersburg, MD. [Online]. Available: http://www.nist.gov/el/isd/ks/upload/NISTSP_1011-I-2-0.pdf

[42] P. Lin, G. Bekey, and K. Abney. (2008). "Autonomous military robotics: Risk, ethics, and design." Prepared for the Department of the Navy, Office of Naval Research. Arlington, Va.

[43] W. Ames. (2004). *Understanding Spyware: Risk and Response.* IT Professional Volume 6, Issue 5. IEEE. [Online]. Available: http://ieeexplore.ieee.org.libproxy.nps.edu/stamp/stamp.jsp?tp=&arnumber=1362621

[44] F. Adib and N. Hajj. (2010). *VSpyware: Spyware in VANETs*. 35th Conference on Local Computer Networks, IEEE. University of Beirut, Lebanon. [Online]. Available: http://ieeexplore.ieee.org.libproxy.nps.edu/stamp/stamp.jsp?tp=&arnumber=5735782

[45] Department of Defense. (2015). *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Joint Chiefs of Staff. Washington, D.C., 2015. Available: http://www.dtic.mil/doctrine/new _pubs/jp1_02.pdf

[46] H. Yilmaz and H. Arslan.(2013). Impersonation attack identification for secure communication. [Online]. Available: http://ieeexplore.ieee.org.libproxy.nps.edu/stamp/stamp.jsp?tp=&arnumber=6825169

[47] M. Srivatsa. (2008). “Who is listening? Security in wireless networks.” *Signal Processing: Communication and Networking*. [Online] Available: http://ieeexplore.ieee.org.libproxy.nps.edu/stamp/stamp.jsp?tp=&arnumber=4447182

[48] I. Qasem, H. Yaghi, and J. Hubbell. (1990). *Computer viruses: Detection and prevention techniques.* [Online]. Available: http://ieeexplore.ieee.org.libproxy.nps.edu/xpl/articleDetails.jsp?tp=&arnumber=117800&queryText%3Dcomputer+viruses

[49] R. Langner. (2011). *Stuxnet: Dissecting a Cyberwarfare Weapon.* [Online]. Available: http://ieeexplore.ieee.org.libproxy.nps.edu/xpl/articleDetails.jsp?tp=&arnumber=5772960&queryText%3DStuxnet

[50] S. Kamal and B. Isaacs. (2007). Analysis of network communication attacks. IEEE. [Online]. Available http://ieeexplore.ieee.org.libproxy.nps.edu/xpl/articleDetails.jsp?tp=&arnumber=4451370&queryText%3DIp+masquerading

[51] J. Anderson and J. Pontus. (2001). *Architectural integration styles for large-scale enterprise software systems.* Enterprise Distributed Object Computing Conference. Seattle, Wa. IEEE. [Online]. Available: http://ieeexplore.ieee.org.libproxy.nps.edu/stamp/stamp.jsp?tp=&arnumber=950442&tag=1

[52] United States Marine Corps. (2011). *Marine Aviation Plan*. Washington, D.C., Department of the Navy.

[53] Department of Defense. (2012). The Role of Autonomy in DOD Systems. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. Washington, D.C., [Online] Available: http://fas.org/irp/agency/dod.dsb/autonomy.pdf

[54] K. Atherton. (2015). For the Second Time Ever a Cyber Attack Causes Physical Damage. Popular Science Online. Retrieved at http://www.popsci.com

[55] Department of the Navy. (2010). EKMS 1B: EKMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 & 3. Washington, D.C., Department of the Navy. [Online]. Available: http://www.public.navy.mil/fcc-c10f/nctsguam/Documents/EKMS-1B_AMD7_Final_23Apr2013.pdf

[56] United States Marine Corps. (2012). *MCWL Campaign Plan*. Washington, D.C., Department of the Navy.

[57] P. Singer, *Wired for War*. New York: Penguin. 2009

[58] United States Marine Corps, *MCRP 4–11.3F: Convoy Operations Handbook.* Quantico, VA: Marine Corps Combat Development Command. 2014

[59] United States Marine Corps, *MCWP 2–25: Ground Reconnaissance Operations DRAFT*. Quantico, VA: Marine Corps Combat Development Command. 2014

[60] United States Marine Corps. (2014). Expeditionary Force 21. Washington, D.C., Department of the Navy.

[61] United States Marine Corps, *MCDP 1: Warfighting*. Washington, D.C., Department of the Navy. 1997

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California